

**АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК
«МОСКОВСКИЙ НАРОДНЫЙ БАНК»
(акционерное общество)**

(АО АКБ «МОСНАРБАНК»)

УТВЕРЖДЕНО

**Протокол заседания Правления
от 01.10.2026 № 49**

**УСЛОВИЯ
использования электронной системы
дистанционного банковского обслуживания**

(Редакция № 4)

**Москва
2026**

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Акт признания Сертификата ключа проверки ЭП для обмена сообщениями (Акт признания) – документ на бумажном носителе, подписываемый Сторонами и удостоверяющий принадлежность приведенного в нем Ключа проверки ЭП и соответствующего ему Ключа ЭП Уполномоченному представителю Клиента (по форме Банка).

Аутентификация – процедура проверки подлинности Клиента/Уполномоченного представителя Клиента с помощью Логина, Пароля, Кодового слова или иным способом, предусмотренным Условиями. Положительный результат Аутентификации подтверждает, что формирование и передача в Банк Электронных документов, а также подтверждение исполнения Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без добровольного согласия Клиента, производится самим Клиентом/Уполномоченным представителем Клиента.

База данных – база данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, формирование и ведение которой осуществляется Банком России в соответствии с законодательством Российской Федерации.

Банк – АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «МОСКОВСКИЙ НАРОДНЫЙ БАНК» (акционерное общество) (полное наименование), АО АКБ «МОСНАРБАНК» (сокращенное наименование), адрес: 121099, г. Москва, ул. Новый Арбат, д. 29, официальный сайт в сети «Интернет»: www.mosnarbank.ru, генеральная лицензия на проведение банковских операций № 2402.

Владелец сертификата ключа проверки ЭП – Клиент, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Закон № 63-ФЗ) порядке выдан Сертификат ключа проверки ЭП.

Временный Пароль – уникальная последовательность символов, передаваемая Клиенту Банком в соответствии с Заявлением на доступ/Заявлением об изменении сведений/Заявлением о Компрометации.

Дистанционное банковское обслуживание (ДБО) – комплекс услуг, предоставляемых Банком Клиенту, предназначенный для осуществления обмена Электронными документами между Клиентом и Банком с использованием Системы в целях проведения на основании Электронных документов банковских операций и сделок согласно установленному Пакету операций; осуществления Банком функций агента валютного контроля;

предоставления в Банк документов, необходимых для осуществления Банком функций, установленных законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма; осуществления переписки между Банком и Клиентом, а также предоставления Сторонами друг другу информации о Счете/Счетах и иных сведений и документов.

Документация – все руководства, инструкции, технические описания и другая документация, касающаяся Системы, которые размещаются Банком в электронном виде на официальном сайте Банка в сети «Интернет» по адресу www.mosnarbank.ru, а также техническое описание организации-разработчика Системы, интегрированное в раздел «Помощь» в Системе.

Договор ДБО – настоящие Условия в совокупности с Заявлением о присоединении к Условиям являются заключенным между Банком и Клиентом Договором об использовании электронной системы дистанционного банковского обслуживания (Договором ДБО).

ЕИО – лицо, являющееся единоличным исполнительным органом Клиента, а также индивидуальный предприниматель и физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой.

Запрос на создание Сертификата ключа проверки ЭП – запрос на регистрацию в Системе Ключа проверки ЭП в электронном виде, который формируется в Системе Уполномоченным представителем Клиента в процессе создания Ключей и направляется в Банк средствами Системы.

Заявление об изменении Соглашения – заявление Клиента на бумажном носителе о распространении Условий на ранее заключенное между Сторонами Соглашение об использовании электронной системы дистанционного банковского обслуживания (по форме Банка).

Заявление о предоставлении права доступа в Систему «Клиент-Банк» (Заявление на доступ) – документ на бумажном носителе, подписываемый Сторонами и подтверждающий факт наделения Уполномоченного представителя Клиента правом на использование Системы в соответствии с Договором ДБО и полномочиями на совершение банковских операций и/или сделок в рамках установленного Пакета операций (по форме Банка).

Заявление о внесении изменений в Договор ДБО – заявление, составленное Клиентом и предназначенное для внесения изменений в Договор ДБО (по форме Банка).

Заявление об изменении сведений об Уполномоченном представителе (Заявление об изменении сведений) – заявление, составленное Клиентом и предназначенное для внесения изменений в информацию об Уполномоченных представителях, предоставленную Клиентом в Банк (по форме Банка).

Заявление о присоединении к Условиям – письменное (на бумажном носителе) волеизъявление Клиента заключить Договор ДБО (по форме Банка).

Квитанция – электронное сообщение о приеме Электронного документа Стороны-отправителя Стороной-получателем или смене статуса документа Стороной-получателем в процессе обработки. Получение Квитанции в Системе влечет за собой смену статуса документа в Системе Стороны-отправителя.

Клиент – юридические лица (включая кредитные организации), индивидуальные предприниматели и физические лица, занимающиеся в установленном законодательством Российской Федерации порядке частной практикой, заключившие с Банком Договор ДБО.

Ключи (Комплект Ключей) – Ключ ЭП и соответствующий ему Ключ проверки ЭП.

Ключ Электронной подписи (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания Электронной подписи.

Ключ проверки Электронной подписи (Ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с Ключом Электронной подписи и предназначенная для проверки подлинности Электронной подписи в Электронном документе. Срок действия Ключа проверки ЭП для УКЭП определяется выпустившим ее Удостоверяющим центром. Срок действия Ключа проверки ЭП для УНЭП, выпущенной Банком, составляет:

- при использовании СКЗИ КриптоПро – 15 (пятнадцать) месяцев с даты формирования Запроса за создание Сертификата ключа проверки ЭП;
- при использовании СКЗИ OpenSSL – 36 (тридцать шесть) месяцев с даты формирования Запроса на создание Сертификата ключа проверки ЭП.

Кодовое слово – последовательность символов, известная только Клиенту и Банку, используемая для Аутентификации Клиента при телефонном разговоре с Клиентом в целях подтверждения/неподтверждения возобновления исполнения операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия

Клиента. Кодовое слово может использоваться многократно. Кодовое слово указывается в Договоре ДБО и может быть изменено в порядке, предусмотренном Условиями.

Компрометация Ключей – возникновение подозрений в том, что используемые Ключи доступны лицам, не имеющим на то полномочий, и/или процессам. К событиям, влекущим за собой Компрометацию Ключей, относятся, включая, но не ограничиваясь, следующие события:

- утрата Носителей с Ключами, в том числе с последующим обнаружением;
- доступ посторонних лиц (не Уполномоченных представителей Клиента) к Ключам;
- сбой (поломка) Носителя с Ключами;
- удаление Ключа ЭП по вине Клиента;
- случаи, когда нельзя достоверно установить, что произошло с Ключом ЭП (в том числе случаи, когда Ключ ЭП/Носитель с Ключами вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий);
- другие события, которые, по мнению Сторон, свидетельствуют о наличии возможности несанкционированного доступа третьих лиц к Ключам.

Логин – уникальная последовательность буквенных/цифровых символов, используемая для Аутентификации Клиента в Системе.

Несанкционированный доступ – наличие оснований полагать, что Система доступна неуполномоченным лицам, независимо от того, нанесен или нет ущерб Банку и/или Клиенту.

К событиям, связанным с Несанкционированным доступом или подозрением на такой доступ, относятся, включая, но не ограничиваясь, следующие события:

- утеря Пароля для входа в Систему;
- доступ к Системе (в том числе к Электронным документам) и ее использование лицами, не имеющими на то полномочий;
- полная или временная утрата контроля доступа к Системе лиц, уполномоченных Клиентом для работы в Системе;
- обнаружение использования Системы без согласия Клиента, а также в случае, если Клиент/Банк подозревает возможность возникновения подобных ситуаций;
- возникновение подозрений на утечку информации или ее искажение в Системе;
- заражение автоматизированного рабочего места Клиента вредоносными программами;
- «хакерская» атака на информационные системы Клиента;

- обнаружение попытки совершения каких-либо иных несанкционированных действий, которые могут привести к сбоям либо иным образом нанести ущерб Клиенту/Банку или другим пользователям Системы.

Носитель с Ключами – съемный/отчуждаемый носитель информации, предназначенный для записи, хранения, воспроизведения Ключей ЭП. Для целей Условий под Носителем с Ключами понимается USB-Токен, USB-флеш-накопитель.

Пакет операций – перечень банковских операций и/или сделок, осуществляемых посредством Системы, вид которого определяется Заявлением о присоединении к Условиям/Заявлением об изменении Соглашения/Заявлением о внесении изменений в Договор ДБО.

Виды Пакетов операций:

«Стандартный» – включает в себя осуществление посредством Системы банковских операций (в том числе расчетных) по Счетам, осуществление депозитарных операций, заключение договоров банковского счета (далее – ДБС) при открытии второго и последующих банковских счетов, заключение договоров банковского вклада (депозита), заключение дополнительных соглашений к Договору ДБО, заключение договора об оказании Банком услуг эквайринга, заключение кредитных договоров (в том числе, но не ограничиваясь, соглашений о предоставлении кредитной линии, кредитных договоров, заключаемых в рамках соглашений о порядке предоставления кредитов) и иных сделок (в том числе, но не ограничиваясь, залог, поручительство, соглашение о предоставлении банковских гарантий, соглашение о порядке предоставления кредитов), предложение (оферта) заключить которые с помощью Системы поступили Клиенту от Банка, а также осуществление операций и действий в соответствии с условиями заключенных между Сторонами ДБС, Договора ДБО и иных соглашений.

«Расчетный» – включает в себя осуществление посредством Системы переводов денежных средств по Счетам в рамках применяемых форм безналичных расчетов, заключение ДБС при открытии второго и последующих банковских счетов, заключение дополнительных соглашений к Договору ДБО, а также совершение других действий в соответствии с условиями заключенных между Сторонами ДБС и Договора ДБО.

«Расчетный Плюс» – включает в себя осуществление посредством Системы переводов денежных средств по Счетам в рамках применяемых форм безналичных расчетов, заключение ДБС при открытии второго и последующих банковских счетов, заключение между Сторонами договоров банковского вклада (депозита), их исполнение и/или расторжение, заключение

дополнительных соглашений к Договору ДБО, а также совершение других действий в соответствии с условиями заключенных между Сторонами ДБС, Договора ДБО и договоров банковского вклада (депозита).

Пароль – уникальная алфавитно-цифровая последовательность символов, известная только Уполномоченному представителю Клиента, соответствующая его Логину и используемая для Аутентификации Уполномоченного представителя Клиента в Системе. Пароль может использоваться многократно.

Плановая смена Ключей – создание Уполномоченным представителем Клиента новых Ключей, которое осуществляется до истечения срока действия действующего Ключа проверки ЭП.

Проверка ЭП Электронного документа – проверка соотношения, связывающего хэш-функцию Электронного документа, ЭП и Ключа проверки ЭП подписавшего абонента. Если такая проверка, произведенная с использованием Средств электронной подписи, даст положительный результат, то ЭП признается правильной, а сам Электронный документ – подлинным, без искажений, в противном случае Электронный документ считается ошибочным, а ЭП под ним – недействительной.

Рабочий день – день, не являющийся нерабочим днем согласно следующему определению. Нерабочими днями считаются субботы и воскресенья (выходные дни), за исключением объявленных рабочими днями в установленном законодательством Российской Федерации порядке, а также нерабочие праздничные дни, установленные Трудовым кодексом Российской Федерации, и те дни, на которые в силу норм законодательства Российской Федерации переносятся выходные дни.

Реестр иноагентов – список иностранных агентов, определенных Федеральным законом от 14.07.2022 №255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием».

Реестр контролируемых лиц – список иностранных граждан или лиц без гражданства, сведения о которых включены в реестр контролируемых лиц в соответствии с Федеральным законом от 25.07.2002 №115-ФЗ «О правовом положении иностранных граждан в Российской Федерации»

Сертификат ключа проверки ЭП – электронный документ или документ на бумажном носителе, выданный Банком/Удостоверяющим центром и подтверждающий принадлежность Ключа проверки ЭП Владелец сертификата ключа проверки ЭП.

Система «Клиент-Банк» (Система) – корпоративная информационная система дистанционного (удаленного) банковского обслуживания, организованная Банком, представляющая собой комплекс программно-технических средств и организационных мероприятий для создания, защиты, передачи и обработки Электронных документов с использованием сети «Интернет». Система используется как электронное средство платежа, а также для обмена Электронными документами между Банком и Клиентом и обеспечивает создание Комплекта Ключей, создание ЭП в Электронном документе, подтверждение подлинности ЭП в Электронном документе.

СБП – сервис быстрых платежей платежной системы Банка России.

Средства обработки и хранения информации – программно-аппаратные средства, требования к которым приведены в Приложении № 1 к настоящим Условиям.

Средства Электронной подписи (Средства криптографической защиты информации) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание Ключа ЭП и Ключа проверки ЭП. Для создания и проверки ЭП, создания Ключей Банком используются сертифицированные криптографические средства защиты информации «КриптоПро», Клиентом используются сертифицированные криптографические средства защиты информации «КриптоПро» (далее – СКЗИ КриптоПро)¹ или криптографические средства защиты информации «OpenSSL» (далее – СКЗИ OpenSSL)². Тип СКЗИ, используемого Клиентом, устанавливается Договором ДБО.

Сторона (Стороны) – Банк и/или Клиент.

Счет – счет, открытый Банком Клиенту на момент заключения Договора ДБО или счета, которые будут открыты Банком Клиенту в будущем, на основании соответствующих ДБС, заключенных между Сторонами.

Тарифы – размеры вознаграждения Банка за оказываемые по Договору ДБО работы и услуги. Тарифы устанавливаются Банком.

Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного

¹ Вывоз полученных Клиентом от Банка СКЗИ КриптоПро с территории Российской Федерации возможен только на основании решения уполномоченного органа/организации в соответствии с законодательством Российской Федерации, при отсутствии указанного решения установка Системы осуществляется по адресу, находящемуся на территории Российской Федерации.

² С возможностью вывоза с территории Российской Федерации без получения соответствующего разрешения уполномоченных органов/организаций в соответствии с законодательством Российской Федерации.

самоуправления, осуществляющие функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Законом № 63-ФЗ.

Уполномоченное лицо Клиента/Банка – ЕИО, а также лицо, действующее от имени и в интересах Клиента/Банка, полномочия которого основаны на доверенности, договоре, акте уполномоченного государственного органа или органа местного самоуправления, законе.

Уполномоченный представитель Клиента – физическое лицо, указанное в Заявлении на доступ и владеющее Ключом ЭП, позволяющим идентифицировать Уполномоченного представителя Клиента в Системе. Уполномоченному представителю Клиента предоставляются следующие права и полномочия:

при выпуске **Ключа ЭП с правом подписи «единственная»**:

- осуществление входа в Систему;
- установление защищенного соединения с Банком для приема и отправки Электронных документов;
- создание любых Электронных документов, предусмотренных установленным Пакетом операций и Договором ДБО;
- создание ЭП в Электронных документах (подписание Электронных документов ЭП) для последующей передачи посредством Системы;
- отправка Электронных документов, подписанных ЭП единолично;
- иные полномочия в соответствии с установленным Пакетом операций и Договором ДБО/доверенностью;

при выпуске **Ключа ЭП с правом подписи «первая»**:

- осуществление входа в Систему;
- установление защищенного соединения с Банком для приема и отправки Электронных документов;
- создание любых Электронных документов, предусмотренных установленным Пакетом операций и Договором ДБО/доверенностью;
- создание ЭП в Электронных документах (подписание Электронных документов ЭП) для последующей передачи посредством Системы;
- отправка Электронных документов, подписанных совместно ЭП с правом подписи «первая» и «вторая»;
- иные полномочия в соответствии с установленным Пакетом операций и Договором ДБО/доверенностью;

при выпуске **Ключа ЭП с правом подписи «вторая»**:

- осуществление входа в Систему;
- установление защищенного соединения с Банком для приема и отправки Электронных документов;

- создание любых Электронных документов, предусмотренных установленным Пакетом операций и Договором ДБО/доверенностью;
- создание ЭП в Электронных документах (подписание Электронных документов ЭП) для последующей передачи посредством Системы;
- отправка Электронных документов, подписанных совместно ЭП с правом подписи «первая» и «вторая»;
- иные полномочия в соответствии с установленным Пакетом операций и Договором ДБО/доверенностью;

при выпуске **Ключа ЭП «без права подписи»:**

- осуществление входа в Систему;
- установление защищенного соединения с Банком для приема и отправки Электронных документов;
- создание любых Электронных документов, предусмотренных Пакетом операций и Договором ДБО;
- отправка Электронных документов, подписанных Уполномоченными представителями Клиента с правом подписи «единственная»/«первая» и «вторая».

При выпуске Банком ЕИО Клиента Ключа ЭП с правом подписи «единственная» или «первая», ЕИО наряду с полномочиями, установленными ему Пакетом операций и Договором ДБО, вправе направлять по Системе документы, необходимые для обновления сведений, полученных в результате идентификации Клиента (его представителей, выгодоприобретателей, бенефициарных владельцев), для открытия и при ведении банковского счета, а также подтверждающие полномочия представителей Клиента, в том числе лиц, наделенных правом подписи (указанных в банковской карточке), за исключением действующего учредительного документа Клиента, выписки из единого государственного реестра юридических лиц, содержащая все сведения о Клиенте (полная выписка), свидетельства о регистрации по месту пребывания, которые должны быть предоставлены за УКЭП уполномоченного государственного органа/его сотрудника, и будут являться надлежащим образом заверенными копиями указанных документов.

Усиленная квалифицированная электронная подпись (УКЭП)³ – электронная подпись, которая соответствует всем признакам усиленной неквалифицированной электронной подписи и следующим дополнительным признакам:

- Ключ проверки ЭП содержится в квалифицированном сертификате;
- для создания и проверки ЭП используются Средства Электронной подписи, получившие подтверждение соответствия требованиям, установленным Законом № 63-ФЗ.

³ Применяется при наличии технической возможности у Банка. Одновременное использование в Системе УКЭП и УНЭП одним Уполномоченным представителем Клиента, являющимся ЕИО, не допускается.

УКЭП выдается Удостоверяющим центром, аккредитованным Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации/Федеральной налоговой службой Российской Федерации, которые осуществляют функции по созданию и выдаче квалифицированных Сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Законом № 63-ФЗ.

Усиленная неквалифицированная электронная подпись (УНЭП) – электронная подпись, выпущенная Банком, которая:

- получена в результате криптографического преобразования информации с использованием Ключа ЭП;
- позволяет определить лицо, подписавшее Электронный документ;
- позволяет обнаружить факт внесения изменений в Электронный документ после момента его подписания;
- создается с использованием Средств Электронной подписи.

Условия СБП – Условия предоставления сервиса по переводу денежных средств в рамках системы быстрых платежей для юридических лиц, утвержденные Банком. Условия СБП публикуются Банком в порядке, предусмотренном п. 14.7 настоящих Условий.

Условия «Контур.Диадок» – Условия юридически значимого электронного документооборота с использованием программы для ЭВМ «Контур.Диадок», утвержденные Банком.

Хэш-функция – алгоритм⁴ вычисления контрольной последовательности для произвольных электронных сообщений с целью доказательной проверки их целостности.

Шифрование – преобразование данных исходных (открытых) сообщений таким образом, что их смысл становится недоступным для любого лица, не владеющего секретом обратного преобразования⁵.

Расшифрование – операция обратная шифрованию.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию, рассматриваемая как аналог собственноручной подписи соответствующего Уполномоченного представителя Клиента. В рамках

⁴ Для СКЗИ КриптоПро – определенный действующим ГОСТом.

⁵ Для СКЗИ КриптоПро – при шифровании используется алгоритм криптографического преобразования действующего ГОСТа.

Условий под Электронной подписью понимается Усиленная неквалифицированная электронная подпись (УНЭП), выпущенная Банком/Усиленная квалифицированная электронная подпись (УКЭП), выпущенная Удостоверяющим центром для ЕИО.

Электронный документ – электронное сообщение, подписанное ЭП, а также платежное требование, требующее получения акцепта Клиента, не подписанное ЭП, и переданное одной из Сторон другой Стороне посредством Системы, в котором информация представлена в электронной форме, равнозначное документу на бумажном носителе, подписанному собственноручной подписью (собственноручными подписями) Уполномоченных лиц Сторон и скрепленному печатью.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Условия использования электронной системы дистанционного банковского обслуживания (далее – Условия) регулируют отношения, возникающие при предоставлении Банком Клиенту услуг ДБО, а также возникающие в связи с этим права, обязанности и ответственность Сторон.

1.2. Условия являются типовыми для всех Клиентов и могут быть приняты Клиентом не иначе как путем присоединения к Условиям в целом в порядке, установленном Условиями.

1.3. Заключение Договора ДБО осуществляется путем присоединения Клиента к Условиям в целом в соответствии со ст. 428 Гражданского кодекса Российской Федерации и производится путем подписания Клиентом Заявления о присоединении к Условиям.

Датой заключения Договора ДБО является дата подписания Банком Заявления о присоединении к Условиям с проставлением на Заявлении о присоединении к Условиям подписи Уполномоченного лица и печати Банка.

Далее положения Условий применяются соответственно установленному Пакету операций.

1.4. Банк вправе отказать Клиенту в заключении Договора ДБО.

Банк отказывает Клиенту в заключении Договора ДБО:

- в случае, если Банком от Банка России получена информация, содержащаяся в Базе данных, которая содержит сведения, относящиеся к Клиенту;
- при обнаружении информации о Клиенте в Реестре иностранных агентов;
- при обнаружении информации об Уполномоченных лицах/Уполномоченных представителях Клиента – иностранных гражданах или лицах без гражданства в Реестре контролируемых лиц;

- в иных случаях, предусмотренных действующим законодательством Российской Федерации.

Банк незамедлительно уведомляет Клиента об отказе в заключении Договора ДБО с указанием причины такого отказа путем направления соответствующей информации с официального адреса электронной почты (e-mail) Банка на официальный адрес электронной почты (e-mail) Клиента, указанный в Заявлении о присоединении к Условиям и (или) полученный в рамках исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма.

1.5. Услуги Дистанционного банковского обслуживания предоставляются Клиентам на основании Договора ДБО.

1.6. Информационный обмен в рамках Системы осуществляется с использованием сети «Интернет».

1.7. Для обеспечения конфиденциальности Электронного документа при передаче с использованием сети «Интернет», а также для обеспечения авторства, целостности и подлинности Электронного документа в Системе Клиентом используется СКЗИ КристоПро или СКЗИ OpenSSL, а Банком – СКЗИ КристоПро.

1.8. Клиент согласен с тем, что использование в Системе СКЗИ OpenSSL/КристоПро в качестве средств обеспечения конфиденциальности при передаче с использованием сети «Интернет», а также для Аутентификации и обеспечения авторства, целостности и подлинности Электронного документа, являются достаточными, т.е. обеспечивающими защиту интересов Клиента.

1.9. Клиент отказывается от предъявления претензий к Банку, основанием которых является использование СКЗИ OpenSSL/СКЗИ КристоПро в качестве средств защиты Электронного документа от несанкционированного доступа при передаче с использованием сети «Интернет», а также для обеспечения авторства и целостности Электронного документа.

1.10. Система используется для обмена Электронными документами в форматах, установленных Системой. Формирование Электронных документов и обмен ими осуществляется в соответствии с требованиями Документации. Любая информация, передаваемая Сторонами по Системе, обрабатывается Средствами криптографической защиты информации.

1.11. Банк, обладая соответствующими правами, предоставленными ему в соответствии с договором, заключенным между Банком и ООО «БСС», предоставляет Клиенту право на пользование Системой в течение действия

Договора ДБО. Право на пользование предоставляется с учетом ограничений, предусмотренных законодательством Российской Федерации о правовой охране программ для ЭВМ.

1.12. На отношения между Банком и Клиентом распространяются Условия СБП (Клиент считается присоединившимся к Условиям СБП), текст которых опубликован в порядке, предусмотренном п. 14.7 настоящих Условий. Банк вправе вносить изменения в Условия СБП в порядке, установленном в Условиях СБП.

1.13. В случае противоречия Условий СБП условиям, изложенным в Договоре ДБО, Условия СБП имеют приоритет.

1.14. Стороны признают, что используемые во взаимоотношениях между ними Электронные документы, подписанные ЭП, в том числе вложения в них, а также платежное требование, требующее получения акцепта Клиента, не подписанное ЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными собственноручными подписями Уполномоченных лиц Сторон и скрепленными печатями, и являются достаточным основанием для выполнения Банком операций, действий, а также для совершения Сторонами сделок.

1.15. Стороны признают, что используемые ими способы доставки, указанные в Приложении № 2 к Условиям, Средства обработки и хранения информации достаточны для обеспечения надежной и эффективной работы по приему, передаче и хранению информации.

1.16. Электронный документ порождает обязательства Сторон по Договору ДБО, ДБС, а также иным соглашениям между Банком и Клиентом, является офертой или акцептом, если он оформлен передающей Стороной в соответствии с Договором ДБО, ДБС, иными соглашениями между Банком и Клиентом, Документацией, а также офертой Банка, подписан ЭП (за исключением случаев, указанных в Условиях) и передан посредством Системы, а принимающей Стороной получен, и Проверка ЭП Электронного документа дала положительный результат.

Электронные документы не могут быть оспорены или отрицаться Сторонами и третьими лицами или быть признаны недействительными только на том основании, что они переданы в Банк с использованием Системы и способов доставки.

1.17. Банк и Клиент используют Систему для передачи Электронных документов друг другу в приоритетном порядке, при этом использование Системы не ограничивает права Клиента по предоставлению в Банк платежных, иных документов на бумажном носителе. Настоящим Стороны соглашаются с тем, что в случае поступления в Банк Электронного документа по Системе и соответствующего платежного, иного документа на бумажном

носителе, содержащих идентичные условия проведения операции, осуществления соответствующих действий, в том числе по Счету, счету депо, счету по вкладу (депозиту) либо поступления в Банк идентичных Электронных документов, Банк будет рассматривать каждый из указанных документов как самостоятельный платежный, иной документ, и осуществит все действия, необходимые для проведения операции, осуществления соответствующих сделок, действий, в том числе по Счету, счету депо, счету по вкладу (депозиту), в соответствии с каждым из представленных/переданных Клиентом документов.

1.18. Внутренние процедуры использования Клиентом Системы и его внутренний документооборот устанавливаются Клиентом самостоятельно.

1.19. Стороны признают в качестве единой шкалы времени при работе с Системой местное время г. Москвы⁶.

1.20. Клиент уведомлен о том, что информация, передаваемая Банком посредством Системы, не является информацией «в реальном времени», за исключением информации об операциях в СБП.

1.21. В целях проведения Банком идентификации представителей Клиента, Клиентом предоставляются в Банк документы, удостоверяющие личность Уполномоченных лиц/Уполномоченных представителей Клиента и/или документы, подтверждающие право иностранных граждан или лиц без гражданства на пребывание (проживание в Российской Федерации). Указанные документы предоставляются в Банк в оригинале или в виде копий, заверенных нотариально (документы, выданные компетентными органами иностранных государств – при условии их легализации). Документы, удостоверяющие личность Уполномоченных лиц/Уполномоченных представителей Клиента также могут быть предоставлены посредством Системы за УНЭП/УКЭП ЕИО или посредством Контур.Диадок⁷ за УКЭП ЕИО и будут являться надлежащим образом заверенными копиями указанных документов.

Для Уполномоченных представителей Клиента с полномочиями «без права подписи» документы, удостоверяющие личность Уполномоченных представителей Клиента и/или документы, подтверждающие право иностранных граждан и лиц без гражданства на пребывание (проживание) в Российской Федерации, могут быть представлены в Банк в копиях, заверенных ЕИО Клиента.

Документы, представляемые Клиентом и составленные на иностранном языке, должны сопровождаться переводом на русский язык, за исключением случаев, установленных законодательством Российской Федерации. Перевод

⁶ Порядок приема и обработки платежей в рамках СБП определен Условиями СБП.

⁷ Как этот термин определен в Условиях «Контур.Диадок».

на русский язык должен быть заверен в порядке, установленном законодательством Российской Федерации.

1.22. В целях проверки полномочий Уполномоченных лиц/Уполномоченных представителей Клиента Клиентом предоставляются в Банк документы, подтверждающие полномочия указанных лиц на совершение банковских операций и/или сделок, осуществляемых посредством Системы в рамках установленного Пакета операций, а также иные необходимые полномочия. Указанные документы могут быть предоставлены в Банк как на бумажном носителе, так и по Системе за УНЭП/УКЭП ЕИО или по Контур.Диадок за УКЭП ЕИО.

При подписании Заявления на доступ/Заявления об изменении сведений ЕИО Клиента документы, подтверждающие полномочия Уполномоченного представителя Клиента на совершение банковских операций и/или сделок, осуществляемых посредством Системы в рамках установленного Пакета операций, а также иные необходимые полномочия, могут не предоставляться, в этом случае полномочия указанных лиц на совершение банковских операций и/или сделок, осуществляемых посредством Системы в рамках установленного Пакета операций, определяются Договором ДБО в рамках установленного Пакета операций без каких-либо ограничений и действительны до исключения Клиентом соответствующего Уполномоченного представителя из состава действующих Уполномоченных представителей Клиента.

1.23. Клиент, ранее заключивший с Банком Соглашение об использовании электронной системы дистанционного банковского обслуживания, вправе заключить с Банком Договор ДБО путем подачи в Банк Заявления об изменении Соглашения. С момента подписания Банком указанного заявления соответствующее соглашение (со всеми изменениями и дополнениями) считается действующим в редакции указанного заявления и Условий, а также считается заключенным между Сторонами новым Договором ДБО (номер Договора ДБО присваивается Банком, датой Договора ДБО считается дата подписания Заявления об изменении Соглашения Банком, отметки о номере и дате соответствующего Договора ДБО проставляются Банком при подписании Заявления об изменении Соглашения).

Указанное в настоящем пункте заявление подается в Банк на бумажном носителе в 2 (двух) экземплярах, один из которых после подписания Банком возвращается Клиенту.

2. ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К СИСТЕМЕ

2.1. Для участия в обмене Электронными документами Клиент выполняет следующие действия:

а) назначает и наделяет соответствующими полномочиями Уполномоченного представителя Клиента;

б) предоставляет в Банк на бумажном носителе 2 (два) экземпляра заполненного Заявления о присоединении к Условиям;

в) для каждого Уполномоченного представителя Клиента предоставляет в Банк на бумажном носителе 2 (два) экземпляра заполненного Заявления на доступ с приложением документов, по форме и содержанию соответствующих п. 1.21, п. 1.22 настоящих Условий;

г) в случае использования УКЭП ЕИО:

- самостоятельно получает в Удостоверяющем центре Средство ЭП и Сертификат ключа проверки УКЭП для ЕИО. Процедура получения УКЭП определяется требованиями Удостоверяющего центра;

- предоставляет в Банк Сертификат ключа проверки УКЭП в электронном виде (на отчуждаемом носителе или путем направления на адрес электронной почты Центра технической поддержки клиентов dbo@mosnarbank.ru (только в заархивированном виде));

д) обеспечивает наличие и приведение оборудования, предназначенного для установки Системы, в соответствии с требованиями к аппаратно-программным средствам, приведенными в Приложении № 1 к Условиям.

2.2. Банк, после принятия от Клиента документов, по форме и содержанию соответствующих подп. б), в) и г) п. 2.1 настоящих Условий, предоставляет Клиенту доступ в Систему и выполняет следующие действия:

а) регистрирует Клиента в Системе;

б) создает в Системе учетные записи Уполномоченных представителей Клиента;

в) передает Клиенту Временные Пароли для входа в Систему в соответствии с Заявлением на доступ;

г) в случае использования УКЭП ЕИО загружает в Систему электронный Сертификат ключа проверки УКЭП, полученный от Клиента, и ограничивает возможность работы с Ключом ЭП сроком действия Сертификата ключа проверки УКЭП, выданного Удостоверяющим центром, при условии совпадения информации о Клиенте, имеющейся в Банке, с информацией, содержащейся в Сертификате ключа проверки УКЭП;

д) проставляет отметки на каждом экземпляре Заявления на доступ и передает один экземпляр указанного заявления Клиенту;

е) проставляет отметки на каждом экземпляре Заявления о присоединении к Условиям и передает один экземпляр указанного заявления Клиенту;

ж) консультирует Клиента по вопросам установки и эксплуатации Системы после проведения Клиентом подготовительных мероприятий, перечисленных в п. 2.1 настоящих Условий.

2.3. Клиент после получения от Банка Временного Пароля выполняет следующие действия:

а) в случае использования УНЭП:

- авторизуется в Системе с помощью Логина и Временного Пароля;

- формирует Ключи и записывает их на свой Носитель с Ключами;
- создает и направляет в Банк по Системе электронный Запрос на создание Сертификата ключа проверки ЭП;
- предоставляет в Банк по каждому из Уполномоченных представителей Клиента Акт признания, распечатанный из Системы, в 2 (двух) экземплярах, подписанный собственноручными подписями Уполномоченного лица Клиента и соответствующего Уполномоченного представителя Клиента;
- б) в случае использования УКЭП ЕИО:
 - авторизуется в Системе с помощью Логина и Временного Пароля;
 - меняет Временный Пароль, полученный от Банка, на свой Пароль.

2.4. Банк (в случае использования УНЭП) после проверки полученного от Клиента надлежащим образом оформленного Акта признания в 2 (двух) экземплярах выполняет следующие действия:

- в течение 2 (двух) Рабочих дней с даты приема Акта признания активирует Ключ проверки ЭП на основании электронного Запроса Клиента на создание Сертификата ключа проверки ЭП;
- проставляет отметку о дате начала и окончания срока действия Ключа проверки ЭП на каждом экземпляре принятого от Клиента Акта признания и передает Клиенту один экземпляр указанного акта.

2.5. Клиент (в случае использования УНЭП) после активации Банком в Системе Ключа проверки ЭП осуществляет следующие действия:

- авторизуется в Системе с помощью Логина и Временного Пароля;
- меняет Временный Пароль, полученный от Банка, на свой Пароль.

2.6. Процесс подключения Клиента к Системе считается завершенным:

а) в случае использования УНЭП – с момента активации Банком в Системе первого Ключа проверки ЭП Уполномоченного представителя Клиента из имеющегося у Клиента набора Ключей, выпущенных Банком одному/нескольким Уполномоченным представителям Клиента;

б) в случае использования УКЭП ЕИО – с момента загрузки Банком в Систему электронного Сертификата ключа проверки УКЭП для ЕИО, полученного от Клиента.

3. ПОРЯДОК ПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ И ПРЕДОСТАВЛЕНИЯ ПРАВА ДОСТУПА В СИСТЕМУ УПОЛНОМОЧЕННОМУ ПРЕДСТАВИТЕЛЮ КЛИЕНТА

3.1. Плановая смена Ключей осуществляется в связи с истечением срока их действия. При Плановой смене Ключей Стороны осуществляют следующие действия:

3.1.1. Клиент:

а) в случае использования УНЭП:

- формирует в Системе новые Ключи и записывает их на свой Носитель с Ключами;

- создает и направляет в Банк электронный Запрос на создание нового Сертификата ключа проверки ЭП;

- предоставляет в Банк на бумажном носителе Акт признания в 2 (двух) экземплярах;

б) в случае использования УКЭП ЕИО самостоятельно получает в Удостоверяющем центре новый Сертификат ключа проверки УКЭП для ЕИО и передает его в Банк в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@mosnarbank.ru (только в заархивированном виде)). Процедура получения УКЭП определяется требованиями Удостоверяющего центра.

3.1.2. Банк:

а) в случае использования УНЭП:

- в течение 2 (двух) Рабочих дней с даты получения от Клиента надлежащим образом оформленного Акта признания в 2 (двух) экземплярах активирует новый Ключ проверки ЭП на основании электронного Запроса Клиента на создание Сертификата ключа проверки ЭП;

- проставляет отметку о дате начала и окончания срока действия Ключа проверки ЭП на каждом экземпляре принятого от Клиента Акта признания и передает Клиенту один экземпляр указанного акта;

б) в случае использования УКЭП ЕИО загружает в Систему новый электронный Сертификат ключа проверки УКЭП, полученный от Клиента, и ограничивает возможность работы с Ключом ЭП сроком действия нового Сертификата ключа проверки УКЭП, выданного Удостоверяющим центром, при условии совпадения информации, имеющейся в Банке, с информацией, содержащейся в Сертификате ключа проверки УКЭП.

3.2. Для предоставления права доступа в Систему новому Уполномоченному представителю Стороны совершают действия, перечисленные в подп. в), г) п. 2.1, подп. б) – д) п. 2.2, п. 2.3 – п. 2.5 настоящих Условий, при этом новый Сертификат ключа проверки УКЭП для ЕИО, полученный Клиентом в Удостоверяющем центре, также может быть передан в Банк посредством Системы.

4. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ДОГОВОР ДБО/ СВЕДЕНИЯ ОБ УПОЛНОМОЧЕННЫХ ПРЕДСТАВИТЕЛЯХ

4.1. В целях внесения изменений в условия Договора ДБО, Клиент, по мере внесения соответствующих изменений, незамедлительно представляет в Банк документы, подтверждающие соответствующие изменения, и Заявление о внесении изменений в Договор ДБО, форма которого размещена на официальном сайте Банка.

В целях внесения изменений в сведения об Уполномоченных представителях, Клиент, по мере внесения соответствующих изменений, незамедлительно представляет в Банк документы, подтверждающие соответствующие изменения и Заявление об изменении сведений, форма которого размещена на официальном сайте Банка.

Случаи предоставления Клиентом вышеуказанных заявлений установлены данными документами.

4.2. Заявление о внесении изменений в Договор ДБО/Заявление об изменении сведений может быть представлено в Банк в 2 (двух) экземплярах на бумажном носителе или направлено по Системе за ЭП Уполномоченного представителя Клиента (при наличии у него соответствующих полномочий).

В случае изменения телефонного номера Клиента, Кодового слова, Заявление о внесении изменений в Договор ДБО предоставляется Клиентом в Банк только на бумажном носителе. Во всех остальных случаях Заявление о внесении изменений в Договор ДБО/Заявление об изменении сведений может быть направлено в Банк посредством Системы в виде вложения в Электронный документ «Письмо в банк» в формате Word или в виде сканированного образа Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений на бумажном носителе, при этом ЭП в Электронном документе «Письмо в банк» и подпись в сканированном образе Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений на бумажном носителе должны принадлежать одному Уполномоченному представителю Клиента.

Датой внесения изменений в Договор ДБО считается дата подписания Банком Заявления о внесении изменений в Договор ДБО с проставлением на нем подписи Уполномоченного лица и печати Банка/направления Банком по Системе письма о принятии (акцепте) Банком Заявления о внесении изменений в Договор ДБО.

В случае поступления Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений в Банк посредством Системы в виде вложения в Электронный документ Банк осуществляет следующие действия:

- при положительном решении о принятии указанных заявлений проставляет в Системе статус «Письмо в банк» «Обработан» с указанием информации о принятии указанных заявлений и дате их принятия, а также направляет Клиенту (в качестве акцепта) по Системе письмо о принятии Заявления о внесении изменений в Договор ДБО;
- при отрицательном решении о принятии указанных заявлений проставляет в Системе статус «Письма в банк» «Отказано» с указанием причины отказа.

4.3. В случае изменения фамилии, имени, отчества (при наличии) Уполномоченного представителя Клиента, Клиент совершает все действия, предусмотренные Условиями для предоставления Уполномоченному

представителю права доступа в Систему, и предоставляет в Банк Заявление об изменении сведений, в котором указывает прежнюю фамилию, имя или отчество (при наличии) соответствующего Уполномоченного представителя.

Банк на основании полученных документов и Заявления об изменении сведений:

- создает в Системе новую учетную запись Уполномоченного представителя Клиента, в которой указывает его новую фамилию, имя или отчество (при наличии);
- осуществляет все действия, предусмотренные Условиями для предоставления Уполномоченному представителю права доступа в Систему;
- аннулирует в Системе учетную запись Уполномоченного представителя Клиента с прежней фамилией, именем, отчеством (при наличии) и блокирует соответствующий Сертификат ключа проверки ЭП.

В случае изменения иных данных Уполномоченного представителя Клиента, Клиент предоставляет в Банк надлежащим образом заверенные копии документов, по форме и содержанию соответствующих п. 1.21 настоящих Условий, и Акт признания в 2 (двух) экземплярах (в случае использования УНЭП), при этом создание нового Комплекта Ключей не требуется.

4.4. В случае прекращения полномочий Уполномоченного представителя, а также при изменении его фамилии, имени или отчества (при наличии), направление Заявления об изменении сведений означает требование Клиента прекратить прием и исполнение любых Электронных документов, подписанных ЭП, сформированной с использованием Ключа ЭП такого Уполномоченного представителя.

4.5. В случае изменения наименования и организационно-правовой формы Клиент:

- при использовании УНЭП: формирует в Системе Запрос на создание Сертификата ключа проверки ЭП, при этом самостоятельно изменяет свое наименование/организационно-правовую форму в Системе, и направляет его в Банк в электронном виде посредством Системы, а также предоставляет в Банк на бумажном носителе Акт признания в 2 (двух) экземплярах;
- при использовании УКЭП ЕИО: самостоятельно получает в Удостоверяющем центре Сертификат ключа проверки УКЭП для ЕИО с новым наименованием/организационно-правовой формой Клиента и передает его в Банк в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@mosnarbank.ru (только в заархивированном виде)).

4.6. В случае смены Средства криптографической защиты информации Банк на основании полученного от Клиента Заявления о внесении изменений в Договор ДБО изменяет в Системе Средство криптографической защиты информации, после чего Клиент (в случае использования УНЭП)

осуществляет действия по созданию Уполномоченному представителю нового Ключа проверки ЭП с использованием соответствующего Средства криптографической защиты информации и предоставляет в Банк Акт признания в 2 (двух) экземплярах в соответствии с подп. а) п. 3.1.1 настоящих Условий.

После получения от Клиента Акта признания Банк осуществляет действия, указанные в подп. а) п. 3.1.2 настоящих Условий.

В случае необходимости использования в Системе УКЭП, выпущенной Удостоверяющим центром для ЕИО, Клиент одновременно с Заявлением о внесении изменений в Договор ДБО предоставляет в Банк Сертификат ключа проверки УКЭП ЕИО в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@mosnarbank.ru (только в заархивированном виде)).

4.7. В случае использования в Системе УКЭП, выпущенной Удостоверяющим центром для ЕИО, вместо УНЭП, ранее выпущенной Банком для ЕИО, Клиент предоставляет в Банк письмо в произвольной форме на бумажном носителе или посредством Системы с приложением Сертификата ключа проверки УКЭП ЕИО в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@mosnarbank.ru (только в заархивированном виде)).

Банк на основании полученного письма Клиента:

- загружает в Систему Сертификат ключа проверки УКЭП ЕИО, полученный от Клиента;
- блокирует в Системе Сертификат ключа проверки УНЭП, выпущенный Банком для ЕИО.

4.8. В случае выпуска Банком УНЭП для ЕИО вместо ранее использовавшейся в Системе УКЭП, выпущенной Удостоверяющим центром для ЕИО, Клиент предоставляет в Банк письмо в произвольной форме на бумажном носителе или посредством Системы.

Банк на основании полученного письма Клиента:

- производит в Системе настройки, позволяющие Клиенту осуществить создание Ключа проверки УНЭП для ЕИО;
- блокирует в Системе Сертификат ключа проверки УКЭП, выпущенный Удостоверяющим центром для ЕИО.

Далее Стороны осуществляют действия, указанные в подп. а) п. 3.1.1 и подп. а) п. 3.1.2 настоящих Условий.

4.9. В целях получения нового Временного Пароля для входа в Систему Клиент запрашивает его в Заявлении о Компрометации в момент уведомления Банка о наступлении события Компрометации либо

предоставляет в Банк Заявление об изменении сведений в порядке, определенном п. 4.2 настоящих Условий.

5. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ И НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ

5.1. В случае Компрометации Ключей и/или Несанкционированного доступа к Системе/к информационным системам Клиента, Клиент обязан незамедлительно уведомить об этом Банк любым возможным способом и направить в Банк Заявление о Компрометации (по форме Банка) вложенным файлом на официальный адрес электронной почты (e-mail) Банка, указанный в Договоре ДБО, с последующим предоставлением в Банк оригинала указанного заявления.

Банк на основании полученного на официальный адрес электронной почты (e-mail) Банка Заявления о Компрометации:

а) при Компрометации Ключей:

- прекращает прием и исполнение любых Электронных документов (полученных, но не исполненных Банком), подписанных ЭП, сформированной с использованием скомпрометированного Ключа ЭП Уполномоченного представителя Клиента;

- приостанавливает использование Системы Уполномоченным представителем Клиента и блокирует скомпрометированный Комплект Ключей указанного Уполномоченного представителя Клиента;

- аннулирует действующий Пароль Уполномоченного представителя Клиента, формирует Временный Пароль и передает его Клиенту способом, указанным в Заявлении о Компрометации;

б) при Несанкционированном доступе к Системе/к информационным системам Клиента:

- прекращает прием и исполнение любых Электронных документов (полученных, но не исполненных Банком);

- приостанавливает использование Системы Клиентом и блокирует Комплекты Ключей всех Уполномоченных представителей Клиента;

- аннулирует действующие Пароли всех Уполномоченных представителей Клиента, формирует Временные Пароли и передает их Клиенту способом, указанным в Заявлении о Компрометации.

Клиент, после получения Временных Паролей и устранения последствий Компрометации Ключей и/или Несанкционированного доступа к Системе/информационным системам Клиента, для восстановления доступа в Систему осуществляет действия, перечисленные в подп. г) п. 2.1, п. 2.3, п. 2.5 настоящих Условий.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6.1. Взаимные права и обязанности Сторон

6.1.1. Стороны при обмене Электронными документами с использованием Системы обязуются руководствоваться правилами и требованиями, установленными законодательством Российской Федерации, ДБО, Договором ДБО, Условиями СБП, иными соглашениями между Банком и Клиентом.

6.1.2. Стороны обязуются не разглашать третьей стороне (за исключением случаев, предусмотренных законодательством Российской Федерации и Договором ДБО) информацию о Средствах криптографической защиты информации, используемых в Системе.

6.1.3. Каждая из Сторон обязуется немедленно информировать другую Сторону обо всех случаях Компрометации Ключей, Несанкционированного доступа к Системе, а также повреждения/утраты программно-аппаратных средств обработки, хранения, передачи Электронных документов, Средств криптографической защиты информации, а также Ключей, и не использовать Ключи при наличии оснований полагать, что они скомпрометированы.

6.1.4. Любые Электронные документы, передаваемые по Системе, подлежат шифрованию.

6.1.5. Любые Электронные документы, передаваемые по Системе, должны быть заверены ЭП Стороны-отправителя, за исключением платежного требования, требующего получения акцепта Клиента, не подписанного ЭП. При этом Стороны согласны, что в этом случае Система используется как способ достоверного определения Банка, направившего такое платежное требование Клиенту.

6.1.6. Клиент уведомлен и согласен, что письмо, направленное Клиентом в Банк в соответствии с Договором ДБО со своего официального адреса электронной почты (e-mail) на официальный адрес электронной почты (e-mail) Банка, считается полученным Банком с момента его регистрации как входящего документа во внутренней системе документооборота Банка.

6.2. Права и обязанности Клиента

6.2.1. Клиент не имеет права тиражировать и передавать третьей стороне программное обеспечение, предоставляемое Банком по Договору ДБО и все конфиденциальные данные, относящиеся к нему.

6.2.2. Клиент имеет право, при необходимости, воспользоваться помощью специалиста Банка по предоставлению права доступа в Систему, направив в Банк письменное заявление.

6.2.3. Клиент обязуется в сроки, предусмотренные Условиями, обеспечить на Счете остаток денежных средств в размере, необходимом для оплаты услуг Банка в соответствии с Договором ДБО и Тарифами.

6.2.4. Клиент обязуется обеспечивать сохранность и целостность установленной Системы, включая Средства криптографической защиты информации, а также выполнять требования к эксплуатации Системы, изложенные в Документации.

6.2.5. Клиент по требованию Банка обязан предоставить заверенные подписями Уполномоченных лиц Клиента и оттиском печати Клиента (при необходимости ее проставления) копии (на бумажном носителе) Электронных документов, переданных по Системе, в течение 5 (пяти) календарных дней с момента направления ему требования.

6.2.6. Клиент обязан незамедлительно информировать Банк об изменении информации, касающейся исполнения Сторонами Договора ДБО, в т.ч. обо всех изменениях в адресах/контактной информации, указанных в Заявлении о присоединении к Условиям/иных документах, предоставленных в Банк в соответствии с Договором ДБО.

6.2.7. Клиент обязан незамедлительно предоставлять в Банк Заявление об изменении сведений при смене ЕИО в целях подтверждения прав действующих Уполномоченных представителей Клиента или изменения их состава, а также при прекращении полномочий действующего Уполномоченного представителя Клиента.

6.2.8. Все риски неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о произошедших изменениях, в том числе, указанных в главе 4, п. 6.2.6, п. 6.2.7, п. 7.10 настоящих Условий, несет Клиент.

6.2.9. Клиент обязан самостоятельно контролировать сроки действия Ключей УНЭП и УКЭП и своевременно инициировать процедуру Плановой смены Ключей до истечения их срока действия.

Информационные уведомления о Плановой смене Ключей размещаются Банком в Системе.

Действие Ключей прекращается, если до истечения срока их действия:

а) Клиентом не направлен в Банк по Системе Запрос на создание Сертификата ключа проверки ЭП и/или не предоставлен в Банк на бумажном носителе Акт признания, а также в случае несоответствия указанного акта, полученного Банком от Клиента на бумажном носителе, положениям настоящих Условий (в случае использования УНЭП);

б) Клиентом не предоставлен в Банк новый Сертификат ключа проверки УКЭП ЕИО в электронном виде (в случае использования УКЭП).

6.2.10. Для возобновления работы в Системе Клиент создает новый Комплект Ключей, после чего Стороны осуществляют действия, предусмотренные п. 3.1 настоящих Условий. При расторжении Договора ДБО

Клиент обязуется уничтожить все предоставленное ему в пользование программное обеспечение (исполняемые и вспомогательные файлы) Системы.

6.2.11. Клиент обязуется не передавать третьим лицам свои права и обязанности по Договору ДБО без письменного согласия Банка.

6.2.12. Клиент обязан проверять наличие новых Электронных документов от Банка, направленных в адрес Клиента, ежедневно, за исключением нерабочих дней Банка, а также ежедневно проверять SMS-сообщения, направленные Банком в связи с выявлением им операций, соответствующих признакам осуществления перевода денежных средств без добровольного согласия Клиента⁸.

Клиент обязан не реже одного раза в 5 (пять) календарных дней знакомиться с информацией, публикуемой Банком в соответствии с п. 14.7 настоящих Условий.

За убытки, возникшие в результате неисполнения Клиентом вышеуказанных обязанностей, Банк ответственности не несет.

6.2.13. Клиент обязуется по требованию и форме Банка предоставлять документы, подтверждающие данные об Уполномоченном представителе Клиента, а также документы, подтверждающие его полномочия на совершение банковских операций и/или сделок, осуществляемых посредством Системы в рамках установленного Пакета операций, а также иные необходимые полномочия.

6.2.14. Клиент обязуется соблюдать требования информационной безопасности при работе с Системой, указанные в Приложении № 4 к Условиям, а также направляемые Банком по Системе и размещаемые на официальном сайте Банка в сети «Интернет».

6.2.15. Клиент обязуется немедленно информировать Банк о направлении Электронных документов по Системе под влиянием обмана или при злоупотреблении его доверием.

6.2.16. В случае использования УКЭП ЕИО Клиент, помимо обязанностей, установленных настоящими Условиями, обязуется:

- самостоятельно получать в Удостоверяющем центре Средство ЭП для создания УКЭП ЕИО;

- самостоятельно контролировать сроки действия Сертификатов ключей проверки ЭП, полученных в Удостоверяющем центре, своевременно производить их замену и предоставлять данную информацию Банку в порядке, предусмотренном настоящими Условиями;

- незамедлительно сообщать Банку о случаях прекращения действия Сертификата ключа проверки ЭП, в порядке, установленном настоящими

⁸ При наличии технической возможности у Банка.

Условиями, и прекратить использование УКЭП ЕИО при направлении Электронных документов в Банк по Системе;

- обеспечивать конфиденциальность Ключей;
- не использовать Ключ ЭП при наличии оснований полагать, что его конфиденциальность нарушена;
- незамедлительно уведомлять Банк и Удостоверяющий центр, выдавший Сертификат ключа проверки ЭП, о нарушении конфиденциальности Ключа ЭП при получении информации о таком нарушении;
- использовать для создания и проверки УКЭП ЕИО, создания Ключей ЭП и Ключей проверки ЭП Средства Электронной подписи, имеющие подтверждение соответствия требованиям, установленным Законом № 63-ФЗ.

6.3. Права и обязанности Банка

6.3.1. Банк не принимает к исполнению Электронные документы, оформленные с нарушением требований законодательства Российской Федерации, Договора ДБО, ДБС, Условий СБП, иных соглашений между Сторонами.

6.3.2. Банк имеет право отказать Клиенту в приеме к исполнению Электронного документа, если Клиент заполнил поля Электронного документа с ошибками. В этом случае Клиенту направляется Квитанция с указанием причины отказа⁹.

6.3.3. Банк не имеет права самостоятельно корректировать реквизиты Электронных документов Клиента.

6.3.4. В случае непредоставления Клиентом документов, указанных в п. 4.3 настоящих Условий, Банк не будет нести ответственность за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, подписанного Уполномоченным представителем Клиента, данные о котором были предоставлены Клиентом в Банк ранее.

6.3.5. Банк прекращает прием/исполнение любых Электронных документов в следующих случаях:

- если они подписаны ЭП, сформированной с использованием скомпрометированного Ключа ЭП Уполномоченного представителя Клиента;
- если они подписаны Ключом ЭП Уполномоченного представителя Клиента после прекращения его полномочий;
- если они подписаны УКЭП в случае прекращения действия Сертификата ключа проверки УКЭП;

⁹ Порядок приема и обработки платежей в рамках СБП определен Условиями СБП.

- в случае прекращения действия аккредитации Удостоверяющего центра, выдавшего Клиенту Сертификат ключа проверки УКЭП.

Все Электронные документы, поступившие в Банк до принятия Банком Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений/Заявления о Компрометации, исполняются в порядке, установленном Условиями или иными соглашениями между Сторонами.

В случае непредоставления оригинала Заявления о Компрометации на бумажном носителе Банк не будет нести ответственность за убытки, причиненные Клиенту в результате прекращения приема и исполнения Электронных документов, подписанных ЭП, сформированной с использованием соответствующего скомпрометированного Ключа ЭП.

6.3.6. Банк имеет право отказать Клиенту в приеме/приостановить исполнение любого Электронного документа по своему усмотрению, в том числе, но не ограничиваясь, в случае возникновения у него подозрений, что Электронный документ подписан не Уполномоченным представителем Клиента, Компрометации Ключей, Несанкционированного доступа к Системе и/или в случае какого-либо нарушения Клиентом Договора ДБО, при этом Клиент вправе передать в Банк соответствующий платежный, иной документ на бумажном носителе¹⁰.

О своем отказе в приеме Электронного документа Банк обязуется уведомить Клиента не позднее Рабочего дня, следующего за днем поступления Электронного документа в Банк, путем направления сообщения Клиенту по Системе.

6.3.7. Банк имеет право отказать Клиенту в приеме Электронных документов/ приостановить их исполнение для проведения расчетных операций по Счету, счету по вкладу (депозиту), подписанных ЭП, а также перевести Клиента в Информационный режим функционирования Системы, при котором Клиенту доступен ограниченный функционал (режим «просмотра», а также направление в Банк сообщений свободного формата), в случаях, предусмотренных законодательством Российской Федерации, в том числе в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

6.3.8. Банк имеет право запрашивать у Клиента подтверждение данных об Уполномоченном представителе Клиента, а также документы, подтверждающие его полномочия на совершение банковских операций и/или сделок, осуществляемых посредством Системы в рамках установленного Пакета операций, а также иные необходимые полномочия.

6.3.9. Банк имеет право заблокировать в Системе Ключ ЭП Уполномоченного представителя Клиента в случае прекращения действия его полномочий до момента предоставления в Банк документов, подтверждающих

¹⁰ Платежные документы в рамках СБП могут передаваться только посредством Системы.

продление его полномочий на новый срок. При продлении полномочий создание новых Ключей ЭП не требуется.

6.3.10. Банк имеет право ограничить право подписи Электронных документов (наделить правом подписи «без права подписи») Уполномоченного представителя Клиента в случае недействительности/истечения срока действия документа, удостоверяющего его личность.

6.3.11. Банк имеет право с учетом полномочий, предоставленных Уполномоченному представителю Клиента, ограничить перечень банковских операций и/или сделок, осуществляемых им посредством Системы.

6.3.12. Банк имеет право вносить в одностороннем порядке изменения в порядок функционирования Системы и сообщать об этом Клиенту в письменном уведомлении на бумажном носителе или посредством Системы.

6.3.13. Банк имеет право приостановить обслуживание Клиента с использованием Системы:

- на время спорных ситуаций с уведомлением об этом Клиента;
- для выполнения неотложных, аварийных и регламентных работ, связанных с обслуживанием Системы.

6.3.14. Банк приостанавливает использование Клиентом Системы при получении от Банка России информации, содержащейся в Базе данных, на период нахождения в ней указанных сведений о Клиенте.

При этом Банк незамедлительно уведомляет об этом Клиента, а также о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России (в том числе через Банк) об исключении сведений, относящихся к Клиенту, из Базы данных.

6.3.15. Банк имеет право по своей инициативе приостановить использование Клиентом Системы при Несанкционированном доступе к Системе.

6.3.16. Банк имеет право по своей инициативе блокировать действие Ключей в случае их Компрометации.

6.3.17. Банк приостанавливает использование Клиентом Системы при получении сведений о нахождении Уполномоченного представителя/Уполномоченного лица Клиента – иностранном гражданине или лице без гражданства в Реестре контролируемых лиц, на период нахождения в нем сведений об указанных лицах Клиента.

6.3.18. Банк информирует Клиента о приостановлении использования Системы (перевод в Информационный режим)/прекращении

использования Системы/блокировке Ключей/ограничении банковских операций и/или сделок, осуществляемых посредством Системы/о возобновлении использования Системы, а также в случаях, предусмотренных законодательством Российской Федерации, с указанием причины такого приостановления/прекращения/ограничения в день такого приостановления/прекращения, ограничения путем направления сообщения по Системе и/или на адрес официальной электронной почты Клиента, указанный в Договоре ДБО или полученный в рамках исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма.

6.3.19. Банк обязуется принимать от Клиента Электронные документы, подписанные Уполномоченным(и) представителем(ями) Клиента в соответствии с условиями Договора ДБО, требованиями законодательства Российской Федерации и осуществлять операции, сделки, иные действия на основании таких Электронных документов в сроки, предусмотренные ДБС, Договором ДБО, Условиями СБП, иными соглашениями между Сторонами, законодательством Российской Федерации.

6.3.20. После подключения к Системе Банк начинает информировать Клиента о совершении каждой операции по Счету, счету депо с использованием Системы или без ее использования путем предоставления Клиенту выписки по Счету, счету депо не позднее Рабочего дня, следующего за днем совершения операции по Счету, счету депо, путем направления их только посредством Системы. Днем выдачи (получения) указанных выписок считается день их направления Банком по Системе. В случае необходимости получения Клиентом выписок по Системе за период до момента подключения к Системе, Клиент вправе обратиться в Банк с соответствующим заявлением, направленным в Банк по Системе либо предоставленным на бумажном носителе.

В случае, если использование Клиентом Системы приостановлено, уведомление Клиента о совершении указанных операций осуществляется путем предоставления Клиенту выписки по Счету, счету депо по Системе незамедлительно после восстановления доступа к ней или другим способом и в сроки, предусмотренные соответствующим ДБС/договором счета депо. Направление Банком указанных выписок по Системе (или другим способом и в сроки, предусмотренные соответствующим ДБС/договором счета депо) является надлежащим уведомлением Клиента о совершении операции с использованием электронного средства платежа в соответствии с законодательством Российской Федерации, и не требует дополнительного направления Банком Клиенту каких-либо иных уведомлений.

6.3.21. Банк обязуется консультировать Клиента по вопросам работы с Системой (с 10.00 до 16.00 московского времени в Рабочие дни), предоставлять Клиенту новые версии Системы, а также информировать

Клиента обо всех изменениях порядка функционирования Системы в течение всего срока действия Договора ДБО.

6.3.22. В целях противодействия осуществлению переводов денежных средств без добровольного согласия клиента, Банк на основании заявления Клиента, составленного по форме Банка на бумажном носителе или направленного с помощью Системы, устанавливает не позднее Рабочего дня, следующего за днем принятия Банком данного заявления:

- соответствующие ограничения (лимиты) по сумме одной операции и/или по общей сумме всех операций за календарный день, проводимых по Счету с помощью Системы;

- соответствующие ограничения по предоставлению Банком Клиенту с помощью Системы кредита либо ограничение максимальной суммы одного кредита и/или кредитов за определенный период времени, определяемые Клиентом.

Отмена установленных ограничений осуществляется Банком после принятия им соответствующего заявления Клиента, представленного в Банк на бумажном носителе.

7. ПРАВА, ОБЯЗАННОСТИ И ПОРЯДОК ДЕЙСТВИЯ СТОРОН ПРИ ВЫЯВЛЕНИИ БАНКОМ ОПЕРАЦИЙ, СООТВЕТСТВУЮЩИХ ПРИЗНАКАМ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА

7.1. Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, обязан при приеме к исполнению распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, приостановить его исполнение на срок, предусмотренный законодательством Российской Федерации.

7.2. О приостановлении исполнения распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, Банк обязуется уведомить Клиента незамедлительно путем направления сообщения Клиенту по своему усмотрению по Системе или по номеру мобильного телефона¹¹, указанному Клиентом в Договоре ДБО или сообщенному Клиентом Банку в порядке, предусмотренном настоящими Условиями.

7.3. Клиент подтверждает/не подтверждает исполнение Банком распоряжения, приостановленного из-за признаков осуществления перевода

¹¹ Клиентам, указавшим при заключении Договора ДБО два номера мобильных телефонов, SMS-сообщение направляется на номер мобильного телефона, указанный в первой строке пункта «Мобильный телефон клиента для приема сообщений в формате SMS-сообщений».

денежных средств без добровольного согласия Клиента, в установленные законодательством Российской Федерации сроки, по номеру телефона Банка, указанному на официальном сайте Банка в сети «Интернет», с произнесением Кодового слова Клиента.

При наличии технической возможности, подтвердить исполнение Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без добровольного согласия Клиента, Клиент может по Системе путем ввода кода-подтверждения, предварительно запрошенного Клиентом по Системе и полученного на номер мобильного телефона, указанный в Договоре ДБО или сообщенный Клиентом Банку в порядке, предусмотренном Условиями. До подтверждения исполнения Банком соответствующего платежа Клиент обязан сверить реквизиты распоряжения, отправленного Клиентом, с реквизитами, указанными в уведомлении, направленном Банком по номеру мобильного телефона, указанному Клиентом в Договоре ДБО или сообщенному Клиентом Банку в порядке, предусмотренном Условиями.

При поступлении, в установленные законодательством Российской Федерации сроки, в Банк подтверждения исполнения Банком соответствующего платежа в течение операционного дня, указанного в ДБС, денежные средства списываются со Счета в текущий Рабочий день Банка. При поступлении вышеуказанного подтверждения после операционного дня, денежные средства списываются со Счета не позднее следующего Рабочего дня Банка.

В случае, если Клиент соглашается с сообщением Банка о том, что операция по Счету соответствует признакам осуществления перевода денежных средств без добровольного согласия Клиента, Клиент вправе незамедлительно направить в Банк отзыв соответствующего распоряжения.

При неполучении, в установленные законодательством Российской Федерации сроки, от Клиента соответствующего подтверждения, Банк отказывает в исполнении распоряжения по истечении данного срока.

Клиент уведомлен о том, что все телефонные разговоры записываются и хранятся в Банке в течение срока, установленного законодательством Российской Федерации. Записи указанных телефонных разговоров могут быть использованы при разрешении любых споров, а также предоставлены в суд.

7.4. В случае, если, несмотря на направление Клиентом подтверждения распоряжения в соответствии с п. 7.3 настоящих Условий, Банк получил от Банка России информацию, содержащуюся в Базе данных, его исполнение приостанавливается Банком на срок, предусмотренный законодательством Российской Федерации.

О приостановлении исполнения подтвержденного распоряжения Банк обязуется уведомить Клиента незамедлительно путем направления сообщения Клиенту по своему усмотрению по Системе или по номеру мобильного

телефона¹², указанному Клиентом в Договоре ДБО или сообщенному Клиентом Банку в порядке, предусмотренном Условиями.

7.5. При неполучении, в установленные законодательством Российской Федерации сроки, от Клиента соответствующего отказа в исполнении Банком подтвержденного распоряжения, по истечении данного срока Банк исполняет подтвержденное распоряжение Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не принимать его к исполнению.

7.6. Днем получения Клиентом сообщений, указанных в п. 7.2 и п. 7.4 настоящих Условий, является день направления Банком указанного сообщения по Системе или день направления Банком SMS-сообщения на номер мобильного телефона Клиента, указанный им в Договоре ДБО или сообщенный Клиентом Банку в порядке, предусмотренном Условиями.

7.7. Клиент подтверждает/не подтверждает исполнение/отказывается от исполнения Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без добровольного согласия Клиента, в Рабочие дни.

7.8. Клиент уведомлен и согласен с тем, что Банк проводит Проверку ЭП Электронного документа (процедуру удостоверения права распоряжения денежными средствами Клиента) каждый раз, когда проводится проверка Электронного документа Клиента на соответствие признакам осуществления перевода денежных средств без добровольного согласия Клиента, а также на наличие информации, содержащейся в Базе данных. В этом случае Банк не несет ответственность за убытки Клиента, которые могут возникнуть у него вследствие неисполнения Электронного документа из-за отрицательного результата Проверки ЭП Электронного документа.

7.9. Банк вправе в одностороннем порядке изменить Кодовое слово Клиента, направив Клиенту уведомление на бумажном носителе с собственноручной подписью руководителя Банка (Уполномоченного им лица) об изменении Кодового слова.

7.10. В случае утраты Клиентом контроля над номером мобильного телефона, а также утраты Клиентом уверенности в том, что Кодовое слово и/или номер мобильного телефона не могут быть использованы неуполномоченными лицами (далее – компрометация), Клиент обязан незамедлительно направить в Банк Заявление о Компрометации (вложенным файлом) на официальный адрес электронной почты (e-mail) Банка, указанный

¹² Клиентам, указавшим при заключении Договора ДБО два номера мобильных телефонов, SMS-сообщение направляется на номер мобильного телефона, указанный в первой строке пункта «Мобильный телефон клиента для приема сообщений в формате SMS-сообщений».

в Договоре ДБО, с последующим немедленным предоставлением в Банк оригинала указанного заявления.

Все распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, поступившие после получения Банком Заявления о Компрометации по электронной почте и до принятия Банком от Клиента последующего Заявления о внесении изменений в Договор ДБО в 2 (двух) экземплярах на бумажном носителе с собственноручной подписью Уполномоченного лица Клиента с указанием нового Кодового слова и/или номера мобильного телефона, считаются автоматически отозванными.

В случае замены Клиентом номера мобильного телефона и/или Кодового слова, Клиент обязан незамедлительно предоставить в Банк Заявление о внесении изменений в Договор ДБО на бумажном носителе в 2 (двух) экземплярах с собственноручной подписью Уполномоченного лица Клиента с указанием нового Кодового слова и/или номера мобильного телефона.

До момента принятия Банком вышеуказанного заявления Банк использует в соответствии с Условиями ранее сообщенный Банку Клиентом номер мобильного телефона, ранее сообщенное Клиентом Банку/Банком Клиенту (в соответствии с п. 7.9 настоящих Условий) Кодовое слово.

7.11. Банк не несет ответственности за ущерб, причиненный Клиенту вследствие несанкционированного использования третьими лицами (в том числе, но не ограничиваясь, при компрометации) Кодового слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента.

7.12. Банк не несет ответственности за негативные последствия, в том числе, убытки Клиента, которые могут возникнуть у Клиента вследствие неполучения уведомлений от Банка об операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, приостановлении исполнения подтвержденного распоряжения или о приостановлении использования Системы, в том числе, в связи с недостоверностью/неактуальностью информации, указанной Клиентом, а также в связи с недоступностью для Клиента указанных способов связи, а также по вине Клиента или мобильного оператора, в случае утраты Клиентом Кодового слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, их компрометации.

7.13. Банк не несет ответственности за убытки Клиента, возникшие в результате утраты (порчи, передачи, утери, разглашении) Клиентом Кодового слова/номера мобильного телефона, на который Банком направляется

SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента.

7.14. Банк не несет ответственности за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку об утрате Клиентом контроля над номером мобильного телефона, а также утрате Клиентом уверенности в том, что Кодовое слово, номер мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, не могут быть использованы неуполномоченными лицами.

7.15. Клиент обязуется предоставить Банку действительный номер мобильного телефона и обеспечить постоянную доступность номера мобильного телефона для приема сообщений в формате SMS-сообщений на русском языке.

7.16. Клиент несет ответственность за достоверность номера мобильного телефона, обязан не допускать создание дубликатов (клонов) sim-карты, а также не допускать получение, использование и замену sim-карты и/или номера мобильного телефона, Кодового слова неуполномоченными лицами.

7.17. Клиент обязуется обеспечить хранение информации о Кодовом слове способом, делающим Кодовое слово недоступным третьим лицам.

Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения невозможности доступа неуполномоченных лиц к информации о Кодовом слове, номере мобильного телефона Клиента, находящейся в распоряжении Банка.

7.18. Клиент подтверждает, что ему известно о том, что в процессе передачи информации путем направления SMS-сообщения возможен риск несанкционированного доступа третьих лиц к такой информации и настоящим выражает свое согласие с тем, что Банк не несет ответственности за разглашение информации о Клиенте, операциях по его Счетам в случае такого несанкционированного доступа.

7.19. Клиент соглашается с тем, что Банк не несет ответственности за какие-либо аварии, сбои и перебои в обслуживании, связанные с оборудованием, системами передачи электроэнергии и/или линий связи, сети «Интернет», которые обеспечиваются, подаются, эксплуатируются и/или обслуживаются третьими лицами в связи с направлением Банком Клиенту SMS-сообщения, в том числе убытки, понесенные в связи с неправомерными действиями или бездействием третьих лиц. Банк не несет ответственность за доступность и работоспособность средств связи, с помощью которых Банк осуществляет уведомление Клиента.

8. КОНФИДЕНЦИАЛЬНОСТЬ

8.1. Условия и информация, содержащаяся в Договоре ДБО, а также вся переписка, связанная с его исполнением, считаются обеими Сторонами конфиденциальной информацией, составляющей, в том числе, банковскую и коммерческую тайну, которую Стороны не вправе разглашать третьим лицам без предварительного письменного согласия другой Стороны, за исключением случаев, предусмотренных Договором ДБО и законодательством Российской Федерации, предоставления такой информации независимым аудиторским организациям по их требованию в ходе проведения аудита бухгалтерского учета и финансовой (бухгалтерской) отчетности, когда она оказалась известной третьим лицам до того, как Стороны ее разгласили.

9. ФИНАНСОВЫЕ ВЗАИМООТНОШЕНИЯ

9.1. Порядок оплаты, стоимость работ и услуг, оказываемых Банком Клиенту по настоящему Договору ДБО, устанавливаются Тарифами и Условиями. Расчеты производятся в рублях путем списания Банком (без дополнительных распоряжений Клиента) денежных средств с расчетного и/или иных счетов Клиента, открытых в Банке, с которых такое списание допускается законодательством Российской Федерации, предварительно полностью до оказания услуг. Если денежные средства списываются со счета Клиента в иностранной валюте, а сумма, причитающаяся Банку в соответствии с Тарифами, выражена в рублях, Банк самостоятельно производит конверсию указанных средств по курсу Банка России на день совершения операции и направляет полученную сумму для оплаты услуг Банка.

9.2. В случае, если остаток денежных средств на расчетном и/или иных счетах Клиента не позволяет Банку в срок и в размере, определенных Договором ДБО и действующими Тарифами, произвести списание платы за услуги Банка, Банк имеет право не оказывать запрашиваемые Клиентом услуги и/или приостановить использование Клиентом Системы до момента полной оплаты задолженности Клиентом, соответственно уведомив об этом Клиента не менее чем за 5 (пять) Рабочих дней. Клиент отказывается от любых претензий к Банку за возникновение в этом случае возможных убытков, включая реальный ущерб и упущенную выгоду, связанных с задержками в проведении Клиентом операций по Счету, счету депо, счету по вкладу (депозиту), осуществления иных действий, сделок.

9.3. В случае расторжения Клиентом Договора ДБО в одностороннем порядке, Клиент обязан не позднее 3 (трех) Рабочих дней от даты направления уведомления о расторжении оплатить стоимость оказанных услуг.

9.4. Клиент настоящим дает согласие (заранее данный акцепт) на исполнение (в том числе, частичное) Банком, в полной сумме платежных требований/инкассовых поручений Банка или иных документов, установленных Банком России, для осуществления прав, предусмотренных п.9.1 настоящих Условий, в течение срока действия Договора ДБО.

10. ОТВЕТСТВЕННОСТЬ СТОРОН

10.1. За неисполнение и/или ненадлежащее исполнение обязательств по Договору ДБО Стороны несут ответственность в соответствии с законодательством Российской Федерации и Договором ДБО.

10.2. Клиент несет ответственность за:

- сохранность и целостность установленного программного обеспечения, включая Средства криптографической защиты информации, Носителей с Ключами;
- выполнение требований к эксплуатации Системы, изложенных в Условиях и Документации;
- надлежащее выполнение условий Договора ДБО, а также за использование Ключей только Уполномоченным представителем Клиента, указанным в соответствующем Заявлении на доступ.

10.3. Банк несет ответственность перед Клиентом в соответствии с законодательством Российской Федерации, при наличии вины за реальный ущерб, но не за упущенную выгоду, с учетом ограничений, предусмотренных п. 10.4 настоящих Условий, за точное, своевременное и полное исполнение поручений и инструкций Клиента по проведению банковских, депозитарных операций, по совершению иных действий, сделок, на основании надлежащим образом оформленных и своевременно переданных по Системе Электронных документов Клиента.

10.4. Банк не несет ответственности:

- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Электронного документа, признанного верным и принятого Банком к исполнению (любой Электронный документ, подписанный ЭП Уполномоченного представителя Клиента в соответствии с Договором ДБО и полученный Банком по Системе, в любом случае признается Электронным документом, исходящим от Клиента, что не допускает отказ Клиента от того, что такой документ направлен с его стороны, ни при каких обстоятельствах);
- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Электронного документа, подписанного прежним Уполномоченным представителем Клиента, до принятия Банком от Клиента Заявления об изменении сведений, касающихся

прекращения полномочий соответствующего Уполномоченного представителя Клиента;

- за последствия отказа Банка в соответствии с п. 6.3.2, п. 6.3.5 – п. 6.3.7 настоящих Условий от приема к исполнению Электронного документа, переданного Клиентом по Системе;

- за последствия использования Системы, установленной у Клиента, посторонними, а также неуполномоченными на это лицами;

- за последствия разглашения Клиентом информации о порядке работы Системы, включая порядок использования Средств криптографической защиты информации;

- за нарушение работы Системы и возникновение трудностей в осуществлении операций, иных действий посредством Системы в результате ошибок и неточностей, допущенных Клиентом;

- за нарушение работы Системы в результате неисправности Средств обработки и хранения информации Клиента, используемых для доступа к Системе;

- за сбои в работе Системы, произошедшие не по вине Банка и повлекшие для Клиента невозможность передачи Электронных документов;

- за нарушение работы Системы в результате действий третьих лиц;

- за последствия нарушения Клиентом требований и правил, приведенных в Договоре ДБО и Документации;

- за последствия нарушения работоспособности телекоммуникационных линий связи, сети «Интернет»;

- за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку о событии Компрометации;

- за убытки, возникшие в результате утраты (порчи, передачи, утери, разглашения) Клиентом применяемых в Системе Паролей, Ключей, Носителей с Ключами, конфиденциальной информации и/или программного обеспечения;

- за правильность заполнения и оформления Электронных документов Клиентом;

- за исполнение ЭД, направленных и подписанных УКЭП Клиента, в случае прекращения Сертификата ключа проверки УКЭП и несообщения данной информации Банку;

- за убытки, возникшие в результате использования Системы в нарушение каких-либо требований законодательства Российской Федерации, применимого к деятельности Клиента;

- за последствия решений органов государственной власти Российской Федерации и других стран, Банка России, которые делают невозможным надлежащее исполнение Банком своих обязательств по Договору ДБО;

- за несанкционированный вывоз Клиентом на территорию иностранного государства СКЗИ КriptoПро.

11. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

11.1. Стороны примут все меры к разрешению всех споров и разногласий, связанных с толкованием Сторонами Договора ДБО и его выполнением, путем переговоров.

11.2. В случае, если Стороны не придут к взаимоприемлемому решению путем переговоров, Сторона, предъявившая претензию, официально вручает другой Стороне уведомление о претензии в письменном виде на бумажном носителе. Сторона, получившая уведомление, проводит расследование по факту претензии в течение 7 (семи) календарных дней от даты получения уведомления, по истечении которых на бумажном носителе уведомляет другую Сторону о результатах расследования.

11.3. В случае, если результаты расследования не удовлетворяют Сторону, предъявившую претензию, либо если такое уведомление не получено Стороной, предъявившей претензию, Стороны формируют Техническую комиссию для разбора конфликтной ситуации в течение 5 (пяти)¹³/15 (пятнадцати)¹⁴ календарных дней с момента истечения срока, указанного в п. 11.2 настоящих Условий. Целью работы Технической комиссии является установление правомерности и обоснованности претензии. Порядок разбора конфликтной ситуации приведен в Приложении № 3 к Условиям. В состав Технической комиссии включаются в равном количестве представители Банка и представители Клиента, а также представители организации-разработчика Системы и, в случае необходимости, независимые эксперты. Их полномочия подтверждаются доверенностями. Лица, входящие в состав Технической комиссии, должны обладать необходимыми знаниями в области обеспечения защиты информации и работы компьютерных информационных систем. Состав Технической комиссии согласовывается Сторонами в акте. Срок действия Технической комиссии составляет не более 14 (четырнадцати) календарных дней.

Стороны согласны с тем, что оплачивать услуги привлеченных экспертов должна Сторона, предъявившая претензию.

11.4. Работа Технической комиссии проходит на территории Банка.

11.5. В случае отсутствия у одной из Сторон каких-либо материалов, требуемых для установления правомерности и обоснованности претензии (перечень материалов приведен в Приложении № 3 к Условиям), спор решается в пользу другой Стороны.

Бремя доказывания лежит на Стороне, заявившей о нарушении ее прав и законных интересов.

¹³ Применимо только для СКЗИ КриптоПро.

¹⁴ Применимо только для СКЗИ OpenSSL.

11.6. Результат работы Технической комиссии оформляется актом, в котором фиксируются выводы, к которым Техническая комиссия пришла в результате проведенных мероприятий, и определяются последующие действия Сторон. Акт подписывается членами Технической комиссии. Стороны признают решение, оформленное актом, обязательным для участников конфликтной ситуации, и обязуются добровольно исполнять решение Технической комиссии в установленные указанным актом сроки.

11.7. Уклонение какой-либо Стороны от участия в создании или работе Технической комиссии может привести к невозможности ее создания и работы, но не может привести к невозможности урегулирования конфликта в судебном порядке. В случае, если Техническая комиссия не будет создана в сроки, предусмотренные Условиями, либо, если в течение 14 (четырнадцати) календарных дней с момента создания Технической комиссии, ее работа не даст результата, либо если Стороны не придут к взаимоприемлемому решению, спор передается на рассмотрение в Арбитражный суд г. Москвы в соответствии с законодательством Российской Федерации.

11.8. Стороны признают, что:

- основополагающим документом при рассмотрении конфликтной ситуации, связанной с обменом Электронными документами посредством Системы, является протокол работы Системы, сформированный Банком;
- Электронные документы, направленные Сторонами друг другу по Системе или хранящиеся в Банке в соответствии с Условиями, а также соответствующие протоколы почтовых серверов и/или сведения из баз данных, фиксирующих отправку каждого уведомления с его содержанием, сформированные на бумажных носителях, подписанные Уполномоченным лицом и скрепленные печатью (при необходимости ее проставления), записи телефонных разговоров между Сторонами являются достаточным доказательством соответствующего факта и могут быть представлены в качестве надлежащего доказательства в суд в случае рассмотрения спора, возникшего в результате применения Системы, а также при рассмотрении споров в досудебном порядке в соответствии с Условиями.

12. СРОК ДЕЙСТВИЯ ДОГОВОРА ДБО

12.1. Договор ДБО действует до момента прекращения обязательств по всем ДБС.

12.2. Банк вправе отказаться от исполнения Договора ДБО полностью в одностороннем порядке, письменно уведомив об этом Клиента, в случае, если по истечении 6 (шести) месяцев с даты заключения Договора ДБО Клиент не выполнил действия, предусмотренные п. 2.3 настоящих Условий (в случае использования УНЭП) или не предоставил в Банк Сертификат ключа проверки УКЭП ЕИО в электронном виде.

12.3. Договор ДБО может быть расторгнут по письменному заявлению одной из Сторон (односторонний отказ от исполнения Договора ДБО полностью).

В случае расторжения Договора ДБО по инициативе Банка, Банк уведомляет об этом Клиента не позднее, чем за 14 (четырнадцать) календарных дней до даты расторжения, с указанием наименования Клиента, причины расторжения, даты и номера Договора ДБО.

В случае расторжения Договора ДБО по инициативе Клиента, Клиент в письменной форме на бумажном носителе уведомляет об этом Банк не позднее, чем за 3 (три) Рабочих дня до даты расторжения.

Расторжение Договора ДБО до истечения срока его действия не освобождает Стороны от выполнения обязательств, предусмотренных Договором ДБО и не исполненных до даты его расторжения, и не лишает Сторону, чьи права по Договору ДБО нарушены в результате невыполнения обязательств другой Стороной, требовать защиты своих прав в соответствии с законодательством Российской Федерации и Договором ДБО.

12.4. Уведомление о расторжении Договора ДБО может быть направлено Банком Клиенту одним или несколькими из нижеперечисленных способов:

- под расписку Уполномоченному лицу Клиента;
- посредством Системы;
- с официального адреса электронной почты (e-mail) Банка на официальный адрес электронной почты (e-mail) Клиента, указанный в Договоре ДБО или полученный в рамках исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма, исключая сведения, содержащие банковскую, коммерческую тайны и персональные данные;
- посредством почтовой/курьерской службы доставки по адресу места нахождения и/или почтовому адресу Клиента или на почтовый адрес, указанный в Договоре ДБО/иных документах, предоставленных в Банк в соответствии с Договором ДБО.

12.5. Банк уведомляет Клиента о прекращении использования им Системы в день расторжения Договора ДБО путем направления сообщения с официального адреса электронной почты (e-mail) Банка на официальный адрес электронной почты (e-mail) Клиента, указанный в Договоре ДБО или полученный в рамках исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма.

12.6. С момента расторжения Договора ДБО на отношения между Банком и Клиентом не распространяются Условия СБП.

13. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

13.1. Стороны освобождаются от ответственности за неисполнение и/или ненадлежащее исполнение обязательств по Договору ДБО, если такое неисполнение явилось результатом действий или обстоятельств непреодолимой силы (далее – Форс-мажор), то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.

13.2. Под термином Форс-мажор понимаются наводнение, пожар, землетрясение, ураган, взрыв, оседание почвы, эпидемии и иные подобные явления, а также война или военные действия в месте нахождения Банка или Клиента, забастовки в отрасли или регионе, принятие органом законодательной, исполнительной или судебной власти акта, повлекшие за собой невозможность надлежащего исполнения Договора ДБО Сторонами.

13.3. Сторона, для которой возникли обстоятельства непреодолимой силы, обязана в течение 7 (семи) Рабочих дней от даты возникновения Форс-мажора уведомить другую Сторону о наступлении таких обстоятельств, с приложением соответствующих доказательств. Доказательством Форс-мажора может служить официальный документ компетентной организации, подтверждающий факт наступления обстоятельств непреодолимой силы.

13.4. В случае наступления обстоятельств непреодолимой силы срок выполнения Сторонами обязательств по Договору ДБО переносится соразмерно времени, в течение которого действуют такие обстоятельства и их последствия. После прекращения действия Форс-мажора обязательства Сторон возобновляются.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1. Если отдельное положение Договора ДБО теряет силу или становится неисполнимым, это не приводит к недействительности других его положений.

14.2. С даты заключения Договора ДБО вся переписка и договоренности между Сторонами, касающиеся условий Договора ДБО и предшествующие его заключению, теряют силу.

14.3. Вся переписка в рамках исполнения Договора ДБО осуществляется Сторонами на русском языке по адресу места нахождения и/или почтовому адресу Стороны, если иной адрес не будет предварительно сообщен любой из Сторон в письменной форме. Сообщения и иная корреспонденция будут направляться Клиенту посредством почтовой/курьерской службы доставки, посредством Системы, путем выдачи Уполномоченному лицу Клиента, а в случаях, установленных Условиями – по электронной почте.

14.4. Документы, связанные с исполнением Банком обязательств по Договору ДБО, направляемые Банком Клиенту по адресу места нахождения Клиента и/или его почтовому адресу, до получения Банком уведомления об их изменении, будут считаться направленными по надлежащему адресу.

14.5. Условия могут быть изменены по инициативе Банка путем внесения изменений и/или дополнений в Условия, в том числе путем утверждения новой редакции Условий, в порядке, установленном настоящим разделом Условий.

14.6. Изменения и/или дополнения в Условия, внесенные Банком, вступают в силу по истечении 5 (пяти) календарных дней с даты опубликования Банком информации об этих изменениях и/или дополнениях либо с даты вступления изменений и/или дополнений в силу, если такая дата указана в опубликованной информации, но не ранее 5 (пяти) календарных дней с даты опубликования информации.

В случае изменения законодательства Российской Федерации Условия, до момента их изменения Банком, применяются в части, не противоречащей требованиям законодательства Российской Федерации.

14.7. Банк с целью ознакомления Клиентов с Условиями публикует их на официальном сайте Банка в сети «Интернет» по адресу: www.mosnarbank.ru.

Моментом публикации Условий, Тарифов и информации для ознакомления Клиентов, в т.ч. Документации, а также моментом ознакомления Клиента с опубликованными Условиями, Тарифами и информацией для ознакомления Клиентов, в т.ч. Документацией, считается момент их первого размещения на официальном сайте Банка в сети «Интернет» по адресу: www.mosnarbank.ru.

14.8. Действие изменений, внесенных в Условия, и вступивших в силу, распространяется на всех лиц, присоединившихся к Условиям, независимо от даты присоединения к Условиям (даты заключения Договора ДБО). В случае несогласия с изменениями, вносимыми в Условия, Клиент вправе расторгнуть Договор ДБО в одностороннем порядке до вступления таких изменений в силу в порядке, установленном в п. 12.3 настоящих Условий.

14.9. В случае, если до вступления в силу опубликованных Банком изменений и/или дополнений, внесенных в Условия, Договор ДБО не расторгнут, Стороны признают, что указанные изменения и/или дополнения в Условия приняты Клиентом.

14.10. Банк не несет ответственности, если информация об изменении и/или дополнении Условий, опубликованная в порядке и в сроки, установленные Условиями, не была получена и/или изучена и/или правильно истолкована Клиентом.

14.11.Для целей Условий Акт признания открытого ключа (сертификата) для обмена сообщениями, подписанный между Сторонами до введения в действие настоящей редакции Условий, признается равнозначным Акту признания Сертификата ключа проверки ЭП для обмена сообщениями.

14.12.Для целей Условий Данные о владельце сертификата ключа проверки ЭП, подписанные Сторонами до введения в действие настоящей редакции Условий, признаются равнозначными Заявлению о предоставлении права доступа.

14.13.Для целей Условий Договоры об использовании электронной системы дистанционного банковского обслуживания, предусматривающие присоединение к Соглашению об использовании электронной системы дистанционного банковского обслуживания (размещенному на официальном сайте Банка в сети «Интернет»), подписанные между Сторонами до введения в действие настоящей редакции Условий, признаются равнозначными Договору ДБО с Пакетом операций «Стандартный».

14.14.Список Приложений, являющихся неотъемлемой частью Условий:

- Приложение № 1 «Требования к аппаратно-программным средствам».
- Приложение № 2 «Способы доставки информации».
- Приложение № 3 «Порядок разбора конфликтных ситуаций».
- Приложение № 4 «Требования информационной безопасности».

ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНЫМ СРЕДСТВАМ

1. Операционная система Windows 7 и выше.
2. Яндекс.Браузер, Chromium-Gost, Chrome, Mozilla или Firefox.
3. Наличие подключенного сетевого или локального принтера.
4. Наличие подключения к сети Internet.
5. Перед установкой Системы необходимо установить программное обеспечение Средства криптографической защиты информации¹⁵.
6. При обмене информацией с бухгалтерскими системами (далее – БС) «1С», «Парус», БЭСТ-4 и с другими БС, в которых есть возможность экспорта документов в текстовый формат, необходимо, чтобы формат дат и чисел импортируемых документов соответствовал форматам дат и чисел, задаваемым в региональных настройках операционной системы компьютера.

¹⁵ Применимо только для СКЗИ КриптоПро.

СПОСОБЫ ДОСТАВКИ ИНФОРМАЦИИ

Работа осуществляется через подключение к своему провайдеру услуг сети «Интернет».

Параметры подключения: открытый TCP порт 443 на сайт <https://corp.mosnarbank.ru>

Параметры подключения могут быть изменены и сообщены Клиенту в письменном уведомлении или направлены Клиенту посредством Системы.

Настройка Клиентом данной транспортной схемы осуществляется на рабочем месте самостоятельно согласно требованиям провайдера.

ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ

1. Общие положения

1.1. В настоящем Порядке под конфликтной ситуацией понимается возникновение у Сторон претензий, связанных с обменом Электронными документами (далее – ЭД) посредством Системы.

1.2. Ниже приведен перечень конфликтных ситуаций по поводу исполнения ЭД, рассматриваемых Технической комиссией, действующей в соответствии с порядком, предусмотренным Условиями:

- ЭД исполнен, а Клиент утверждает, что ЭД не посылал и не подписывал;
- Клиент утверждает, что он направил ЭД, а ЭД не исполнен, причем, по утверждению Клиента, от Банка получена Квитанция об исполнении;
- Клиент утверждает, что он направил один ЭД, а исполнен другой ЭД;
- не подтверждена подлинность ЭД средствами проверки ЭП принимающей Стороны;
- оспаривается факт идентификации Уполномоченного представителя Клиента, которому предоставлено право подписания от имени Клиента направляемых в Банк ЭД;
- другие конфликтные ситуации, связанные с функционированием Системы.

1.3. При возникновении разногласий Сторон в связи с обменом ЭД посредством Системы, а также в иных случаях возникновения конфликтных/спорных ситуаций, связанных с эксплуатацией Системы, обмен ЭД немедленно прекращается.

1.4. До разрешения конфликтной ситуации Клиенту рекомендуется не использовать в работе персональный компьютер, на который установлено программное обеспечение Системы.

1.5. При разрешении конфликтных ситуаций Стороны обязуются руководствоваться следующими принципами:

- Сторона-получатель обязуется признать подлинным и действительным ЭД, переданный ей посредством Системы и имеющий ЭП, сформированную на Ключах ЭП Стороны-отправителя, при условии положительного результата проверки ЭП на соответствующих им Ключах проверки ЭП;
- Сторона-отправитель обязуется признать подлинным (переданным ею посредством Системы) и действительным ЭД, имеющий ЭП,

сформированную на ее Ключах ЭП, при условии положительного результата проверки ЭП на соответствующих им Ключах проверки ЭП;

- ответственность возлагается на Сторону-отправителя при получении Стороной-получателем ложного ЭД с успешно подделанной ЭП, так как в этом случае Сторона-отправитель не обеспечила сохранность Ключей ЭП.

1.6. Стороны признают, что математические свойства алгоритма ЭП¹⁶ гарантируют невозможность подделки значения ЭП любым лицом, не обладающим Ключом ЭП.

1.7. Стороны должны представить Технической комиссии следующие материалы:

- уведомление о претензии в письменном виде на бумажном носителе с подробным изложением обстоятельств и предполагаемых причин возникновения конфликтной ситуации;

- носители информации с файлами, содержащими спорный ЭД, выгруженный из Системы, а также распечатанный из Системы спорный ЭД на бумажном носителе или Квитанция на него. Описание процедуры выгрузки данных для проверки ЭП приведено в Документации;

- выписка из протокола работы Системы, подтверждающая прием/отправку спорного ЭД, на бумажном носителе, за согласованный Сторонами период;

- в случае использования УНЭП: подписанные собственноручными подписями Уполномоченных лиц Сторон оригиналы Актов признания;

- в случае использования УКЭП: Сертификат ключа проверки УКЭП, выданный Удостоверяющим центром, подтверждающий факт действительности ЭП под оспариваемым ЭД;

- оригиналы заявлений об изменении состава Уполномоченных представителей Клиента, аннулировании действия Ключа проверки ЭП Уполномоченного представителя Клиента (при наличии);

- Ключ проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка, с помощью которых проводилась проверка ЭП оспариваемого ЭД;

- распечатки Ключа проверки УНЭП/Сертификата ключа проверки УКЭП Клиента, распечатку Ключа проверки УНЭП Уполномоченного лица Банка на бумажном носителе;

- Носители с Ключами;

- другие материалы, имеющие отношение к сути рассматриваемой претензии.

1.8. Стороны обязаны способствовать работе Технической комиссии и не допускать необоснованного отказа от предоставления необходимых документов. В случае непредоставления в установленный срок Технической комиссии одной из Сторон каких-либо из вышеперечисленных материалов к

¹⁶ Для СКЗИ КриптоПро – реализованного в соответствии с требованиями стандартов Российской Федерации действующих ГОСТов.

рассмотрению принимаются аналогичные материалы, предоставленные другой Стороной.

2. Процедура проверки подлинности Электронных документов

2.1. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.

2.2. При разборе конфликтных ситуаций используется стороннее эталонное программное обеспечение проверки подлинности ЭП и Сертификатов ключа проверки ЭП.

2.3. Проверка подлинности ЭП под спорным ЭД Клиента осуществляется посредством:

- программного средства «КриптоАРМ», установленного в Банке¹⁷ либо

- программы OpenSSL.exe¹⁸. Описание программы приведено в документации на официальном сайте разработчика в сети «Интернет»: <http://openssl.org/docs/>.

2.4. Проверка подлинности ЭП под спорным ЭД Банка осуществляется посредством программного средства «КриптоАРМ», установленного в Банке.

2.5. Процедура проверки Технической комиссией УНЭП, выпущенной Банком/УКЭП, выпущенной в соответствии с внутренним регламентом Удостоверяющего центра, под спорным ЭД включает следующие действия:

- установление времени подписания и отправки оспариваемого ЭД Уполномоченным представителем Клиента/Уполномоченным лицом Банка;

- сверка даты и времени регистрации, а также срока действия Ключей проверки ЭП Уполномоченного представителя Клиента/Уполномоченного лица Банка, подписавших спорный ЭД, с датой и временем подписания спорного ЭД;

- сверка даты и времени регистрации в Банке заявлений об изменении состава/аннулировании действия ключей ЭП Уполномоченных представителей Клиента, подписавших спорный ЭД (при наличии), с датой и временем подписания спорного ЭД;

- проверка действительности полномочий лиц, подписавших спорный ЭД, на дату его подписания, осуществляемая по результатам рассмотрения соответствующих документов, подтверждающих их полномочия;

- проверка подлинности УНЭП/УКЭП под выгруженным спорным ЭД с использованием Ключа проверки ЭП Стороны-отправителя спорного ЭД;

- проверка подлинности и целостности Ключей проверки ЭП Уполномоченных представителей Клиента/Уполномоченных лиц Банка:

- В случае использования УНЭП:

- проверка соответствия экземпляров Актов признания, предоставленных Сторонами в соответствии с п. 1.7 настоящего Порядка;

¹⁷ Применимо только для СКЗИ КриптоПро.

¹⁸ Применимо только к СКЗИ OpenSSL.

- сверка соответствия ключевых полей Ключа проверки ЭП из Актов признания с распечаткой протокола проверки ЭП, полученной при помощи программы OpenSSL.exe¹⁹/посредством программного средства «КриптоАРМ»²⁰, установленного в Банке.

- В случае использования УКЭП:

- сверка соответствия ключевых полей Ключа проверки ЭП из файла Сертификата ключа проверки УКЭП, направленного Клиентом в Банк, с распечаткой протокола проверки ЭП, полученной посредством программного средства «КриптоАРМ»²¹, установленного в Банке;

- в случае необходимости подтверждения УКЭП Техническая комиссия направляет запрос в Удостоверяющий центр о подтверждении действительности УКЭП на дату подписания оспариваемого ЭД.

2.6. Подтверждением корректности УНЭП/УКЭП под оспариваемым ЭД является одновременное выполнение следующих условий:

- Ключи проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка, с помощью которых проверялись УНЭП/УКЭП, в момент поступления ЭД в Банк/Клиенту и его проверки являлись действующими, т.е. были зарегистрированы в установленном Банком или внутренним регламентом работы Удостоверяющего центра порядке, сроки их действия не истекли, и они не были отменены;

- подтверждена подлинность и целостность Ключей проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка, с помощью которых проводилась проверка УНЭП/УКЭП;

- проверка УНЭП/УКЭП под спорным ЭД с использованием Ключей проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка дала положительный результат, то есть подтвердила подлинность УНЭП/УКЭП под спорным ЭД;

- действия Банка по обработке ЭД проведены в соответствии с информацией, содержащейся в ЭД.

2.7. В случае выполнения всех условий, перечисленных в п. 2.6 настоящего Порядка, Стороны соглашаются с тем, что корректность УНЭП/УКЭП под оспариваемым ЭД подтверждена, то есть проверяемый ЭД подписан корректными УНЭП/УКЭП.

2.8. В случае невыполнения любого из условий, перечисленных в п. 2.6 настоящего Порядка, Стороны соглашаются с тем, что корректность УНЭП/УКЭП не подтверждена, то есть проверяемый ЭД подписан некорректными УНЭП/УКЭП.

2.9. В том случае, если Банк принял к исполнению ЭД, подписанный УНЭП/УКЭП Уполномоченного представителя Клиента, корректность которого установлена Технической комиссией (Стороны согласны с выводами Технической комиссии), Стороны соглашаются с тем, что претензии Клиента

¹⁹ Применимо только к СКЗИ OpenSSL.

²⁰ Применимо только к СКЗИ КриптоПро.

²¹ Применимо только к СКЗИ КриптоПро.

к Банку, связанные с последствиями исполнения указанного ЭД, являются необоснованными.

2.10. В том случае, если Банк принял к исполнению ЭД, подписанный УНЭП/УКЭП Уполномоченного представителя Клиента, корректность которого не подтверждена Технической комиссией (Стороны согласны с выводами Технической комиссии), претензии Клиента к Банку, связанные с последствиями исполнения указанного документа признаются обоснованными.

2.11. Результаты работы Технической комиссии отражаются в акте, составленном в 2 (двух) экземплярах, по одному экземпляру для каждой Стороны, и являющимся основанием принятия Сторонами окончательного решения об урегулировании конфликтной ситуации.

Акт о результатах проведения технической экспертизы должен содержать следующую информацию:

- состав Технической комиссии;
- дата и место составления акта;
- дата и время начала и окончания работы Технической комиссии;
- суть претензии;
- перечень мероприятий, проведённых Технической комиссией;
- фактические обстоятельства, установленные Технической комиссией;
- выводы, к которым пришла Техническая комиссия в результате проведённых мероприятий;
- подписи членов Технической комиссии на каждом листе акта.

2.12. Акт подписывается всеми членами Технической комиссии. Члены Технической комиссии, не согласные с выводами большинства, подписывают акт с возражениями, который прилагается к основному акту, либо излагают свое несогласие и выводы в письменном виде в отдельном документе, который прилагается к основному акту.

2.13. В случае несогласия одной из Сторон с выводами Технической комиссии, отражёнными в акте о результатах проведения технической экспертизы, уклонения от формирования Технической комиссии либо участия в её работе, препятствования участию второй Стороны в работе Технической комиссии, вторая Сторона вправе передать спор на рассмотрение в Арбитражный суд г. Москвы.

ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для минимизации рисков Несанкционированного доступа к Системе, к Счетам, счету по вкладу (депозиту) Клиента со стороны злоумышленников и компрометации ключевой информации, Банк настоятельно просит Клиентов соблюдать следующие меры информационной безопасности:

- Выделить отдельный компьютер, который не будет использоваться в иных целях, кроме как для установки и работы в Системе, и предоставить доступ к нему ограниченному кругу лиц.
- Не осуществлять, а при наличии технической возможности, запретить выход в сеть «Интернет» с этого компьютера на иные адреса, за исключением адресов серверов Банка.
- Ограничить или полностью запретить удаленный доступ к выделенному компьютеру с других компьютеров локальной сети. Не использовать средства удаленного администрирования на выделенном компьютере. При наличии технических средств, поместить выделенный компьютер в отдельную сеть, контролируруемую межсетевым экраном и системами обнаружения атак.
- Заменить все стандартные Пароли, заданные при установке Системы, на уникальные собственные, производить периодическую смену Паролей (не реже одного раза в три месяца); не оставлять в легкодоступных местах и не передавать неуполномоченным лицам записи, содержащие сведения о Паролях для входа в Систему, хранить записи о Паролях в месте, защищенном от несанкционированного доступа.
- Использовать на постоянной основе антивирусное программное обеспечение с последней актуальной версией баз.
- Регулярно (не реже одного раза в неделю) выполнять антивирусную проверку для своевременного обнаружения вредоносных программ.
- Использовать на компьютере исключительно лицензионное программное обеспечение.
- Регулярно (не реже одного раза в месяц или по факту публикации) устанавливать обновления операционной системы.

- Проверить группу «Администраторы» на выделенном компьютере, исключить всех рядовых пользователей из этой группы, не работающих с Системой.
- При наличии технической возможности, для пользователей, работающих с Системой, создать отдельную групповую политику, разрешающую запуск только определенных приложений.
- Для доступа к серверам Банка использовать только заведомо известные Вам адреса интернет серверов Банка.
- В случае отсутствия возможности подключения к серверу Банка незамедлительно сообщать об этом Банку.
- Хранить в безопасном месте (в сейфе) и никому не передавать Носители с Ключами электронной подписи и Ключами проверки электронной подписи (далее – Ключи), обеспечив к ним доступ только Уполномоченных представителей.
- Никогда не осуществлять копирование Ключей на локальный жесткий диск компьютера, даже с последующим его удалением.
- Регулярно (не реже одного раза в месяц) проверять целостность Носителей с Ключами, проводя проверку наличия на них файлов электронной подписи.
- Своевременно (в соответствии с положениями Условий) проводить Плановую смену Ключей.
- Не оставлять Носители с Ключами без присмотра, подключать их к компьютеру только на время использования и незамедлительно их отключать после проведения банковских операций. При оставлении рабочего места Системы без присмотра всегда блокировать экран с последующим вводом пароля для его разблокировки.
- Производить незамедлительную замену Ключей в случае их компрометации или подозрении на компрометацию.
- Принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства на компьютере и в Системе, появление на компьютере и в Системе компьютерных вирусов, а также программ, направленных на разрушение и модификацию программного обеспечения Системы, Электронных документов, либо на перехват Паролей, Ключей и другой конфиденциальной информации.
- Своевременно устанавливать все обновления Системы.

- Не устанавливать обновления, а также не открывать ссылки в почтовых сообщениях, полученных от имени Банка по электронной почте; получив такое сообщение, незамедлительно сообщать об этом Банку.
- Ежедневно, в течение операционного дня Банка и по окончании Рабочего дня, осуществлять дополнительный вход в Систему для контроля перечня исходящих документов за текущий день. При обнаружении подозрительных документов, незамедлительно обращаться в Банк.
- В случае подозрений на замедление работы компьютера отключить компьютер физически от локальной сети и сети «Интернет» и обратиться к системному администратору с просьбой о необходимости проведения полной антивирусной проверки сканированием всех файлов и памяти компьютера.
- В случае, если инцидент информационной безопасности все же произошел, ни в коем случае не выключать компьютер, а отключить его физически только от локальной сети и сети «Интернет», незамедлительно обратиться к системному администратору и сообщить об инциденте в Банк.
- В случае выявления Клиентом подозрительных операций в Системе незамедлительно сообщать об этом в Банк.